(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年1 月10 日 (10.01.2002)

PCT

(10) 国際公開番号
WO 02/03215 A1

(51) 国際特許分類[7]: G06F 15/00, 12/14, 12/00

(21) 国際出願番号: PCT/JP01/05655

(22) 国際出願日: 2001 年6 月29 日 (29.06.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-200210 2000 年6 月30 日 (30.06.2000) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府門真市大字門真1006番地 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 佐久嶋ひろみ (SAKUSHIMA, Hiromi) [JP/JP]; 〒213-0001 神奈川県川崎市高津区溝口6-8-7-304 Kanagawa (JP). 浦中祥子 (URANAKA, Sachiko) [JP/JP]; 〒113-0021 東京都文京区本駒込3-13-8 Tokyo (JP).

(74) 代理人: 工藤一郎(KUDO, Ichiro); 〒100-0006 東京都千代田区有楽町1-8-1 日比谷パークビル Tokyo (JP).

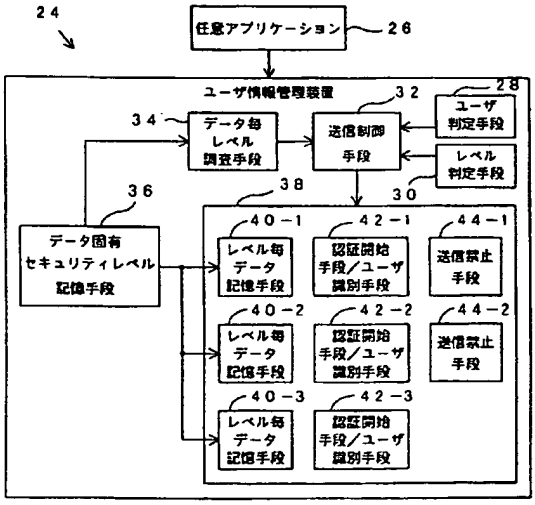
(81) 指定国 (国内): DE, GB, JP, US.

(84) 指定国 (広域): ヨーロッパ特許 (DE, FR, GB).

添付公開書類:
— 国際調査報告書

(54) Title: USER INFORMATION CONTROL DEVICE

(54) 発明の名称: ユーザ情報管理装置



24...USER INFORMATION CONTROL DEVICE
26...ARBITRARY APPLICATION
28...USER JUDGING MEANS
30...LEVEL JUDGING MEANS
32...TRANSMISSION CONTROL MEANS
34...DATA-BY-DATA LEVEL INVERSTIGATING MEANS
36...DATA-SPECIFIC SERCURITY LEVEL STORING MEANS
40-1...LEVEL-BY-LEVEL DATA STORING MEANS
40-2...LEVEL-BY-LEVEL DATA STORING MEANS
40-3...LEVEL-BY-LEVEL DATA STORING MEANS

42-1...AUTHENTICATION STARTING MEANS/USER IDENTIFYING MEANS
42-2...AUTHENTICATION STARTING MEANS/USER IDENTIFYING MEANS
42-3...AUTHENTICATION STARTING MEANS/USER IDENTIFYING MEANS
44-1...TRANSMISSIO INHIBITING MEANS
44-2...TRANSMISSIO INHIBITING MEANS

(57) Abstract: A user information control device capable of protecting security by effectively preventing user information from being used by the other members of a family or flowing out to the outside, a user information control method, a recording medium having a control program for user information control recorded thereon, and a user information control program, wherein transmission inhibiting means (44-1, 44-2) are provided that disable the transmission of specified transmission-enabled user information after elapse of a predetermined time and/or execution of specified operations or according to a specific instruction from the user, subsequent to the transmission-enabling of the specified user information by a transmission control means. In addition, a prudent information control is made possible by controlling personal information that should be controlled according to ranks or levels by classifying it into segments at specified levels.

[続葉有]

WO 02/03215 A1

(57) 要約:

ユーザ情報が家族の他の者に利用されたり、外部に流出することを効果的に防止してセキュリティを保護することの可能なユーザ情報管理装置、ユーザ情報管理方法、ユーザ情報管理のための制御プログラムの記録された記録媒体、及び、ユーザ情報管理プログラムを提供するために、所定のユーザ情報が送信制御手段により送信可能とされた後、所定時間の経過及び／又は所定動作の実行後に、あるいは前記ユーザからの所定の指示に応じて前記送信可能とされたユーザ情報を送信不可能な状態とする送信禁止手段４４－１、４４－２を設けたものである。また、上記ランクやレベルを付けて管理したい個人情報などを、所定のレベルなどに分類して管理できるようにすることにより、きめ細かな情報管理を行うことが可能となる。

明細書

ユーザ情報管理装置

技術分野

本発明は、ユーザ情報のセキュリティ保護に関し、特に双方向通信機能を有するユーザ端末及び／又はこれに接続されるサーバに保持されるユーザに関する情報のセキュリティ保護のためのユーザ情報管理装置、ユーザ情報管理方法、ユーザ情報管理方法を実行するための制御プログラムの記録された記録媒体、及び、ユーザ情報管理プログラムに関する。

背景技術

従来の双方向通信は、主としてユーザ端末としてパーソナルコンピュータ（パソコン）が用いられている。かかるパソコン環境における情報のセキュリティについては、１つの端末が１人のユーザにのみ利用されることが想定され、かかる想定の下でログイン／ログアウトによるセキュリティ管理が基本となっている。しかし、デジタルテレビ端末では、家族の複数の人が同時に１台のテレビを見たり、情報を発信したり、また明確なログイン／ログアウトなどをしないまま他のユーザとが利用する形態が想定される。

すなわち、家族の一人がデジタルテレビ端末を用いてサーバ経由でオンラインショッピングをしたとき、商品の購入に必要なクレジットカードの番号や有効期限などの個人情報あるいはユーザ端末情報がユーザ端末やサーバに保持された状態が継続している。この状態で、商品を購入した人がデジタルテレビ端末から離れていると、家族の他の者が最初の購入者の意志に拘わらず、その最初の購入者のクレジットカードなどの

情報を用いて更に商品の購入をしてしまうことが予想される。また、家族による個人情報の悪用のみならず、個人情報あるいはユーザ端末情報がユーザ端末やサーバに保持された状態が継続していると、かかる情報が不用意に外部に流出する危険もある。また、個人情報には、クレジットカードの番号などのように財産や金品に関連する重要なものと、氏名や性別などのように他人には知られたくないが、極めて秘密性が高いものではないものなど、ランクやレベルを付けて管理したいものもある。なお、公知のセキュリティ技術としては、Java2(http://java.sun.com/)によるセキュリティのように、アプリケーション又はクラスがどんなリソース（ファイル）に対してどんなアクション（読み、書き）を実行できるかを指定するやりかたや、Ｐ３Ｐ(http://www.w3.org/P3P/)のように、Webサイトへのアクセスに対し個人別のアクセスポリシー（プリファレンス）とサイトのポリシーを比較しアクセスするか否かを判断するものがある。

しかし、これらを複数のユーザが利用する端末における上記個人情報のセキュリティ対策に用いたとしても十分な効果を発揮することができないという問題があった。さらに、特開２０００－１１２７９６号公報に示される技術で、データベース表に格納されているプライバシーパラメータにしたがってデータベースへのアクセスを制御するものがある。この技術では、プライバシーパラメータの適用を有効にするため、監査モジュールを含むことが必要であり、全てのデータが通過する複数の強制データビューを有するものである。

したがって、本発明はユーザ情報が家族の他の者に利用されたり、外部に流出することを効果的に防止してセキュリティを保護することの可能なユーザ情報管理装置及びユーザ情報管理方法並びにユーザ情報管理のための制御プログラムの記録された記録媒体を提供することを目的と

する。また、上記ランクやレベルを付けて管理したい個人情報などを、所定のレベルなどに分類して管理できるようにすることは本発明の好ましい態様である。

また、従来のログイン／ログアウトによるセキュリティ管理では、あるデータにアクセスしようとして、そのデータに対するアクセス権限がなくエラーが起きた場合には、アクセス権限を獲得するために、アクセス権限を持つユーザにログインを行わなければいけないが、ログインを行った後で、再度同じ操作を行って同じデータへアクセスすることが必要となり、今まで行った操作を無駄にしないで、スムーズにアクセス権限だけを変更することができなかった。

したがって、データに対するアクセスが受け付けられ、アクセス権限がないことによるエラーが発生しても、受け付けられたアクセスのデータに対するアクセス権限を変更し、操作を続行するようにすることは、本発明の好ましい態様である。

発明の開示

本発明は、このような目的を達成するために、本発明では所定のユーザ情報が送信制御手段により送信可能とされた後、所定時間の経過及び／又は所定動作の実行後に、あるいは前記ユーザからの所定の指示に応じて前記送信可能とされたユーザ情報を送信不可能な状態とする送信禁止手段を設けたものである。また、上記ランクやレベルを付けて管理したい個人情報などを、所定のレベルなどに分類して管理できるようにすることにより、きめ細かな情報管理を行うことが可能となる。

すなわち本発明によれば、ユーザ端末と双方向通信が可能なサーバ上に、あるいは前記ユーザ端末に構築されたユーザ情報管理装置であって、前記ユーザ端末を利用する複数のユーザに関するユーザ情報をセキュリ

ティレベルと関連づけて保持するための記憶手段と、前記ユーザが前記サーバにアクセスして、所定のアプリケーションを利用しようとしたとき、前記ユーザを識別する識別手段と、前記ユーザが前記サーバにアクセスしたとき、あらかじめ定められた複数の認証レベルのいずれの認証レベルであるかを判定するレベル判定手段と、前記記憶手段に保持されている前記ユーザ情報の中で、前記判定されたレベルに対応する前記セキュリティレベル及びそれ以下のセキュリティレベルのユーザ情報のみを前記ユーザ端末及び／又は他の装置に対して送信可能とする送信制御手段と、前記送信制御手段により送信可能とされた後、所定時間の経過及び／又は所定動作の実行後に、あるいは前記ユーザからの所定の指示に応じて前記送信可能とされたユーザ情報を送信不可能な状態とする送信禁止手段とを、有するユーザ情報管理装置が提供される。

また本発明によれば、ユーザ端末と双方向通信が可能なサーバ上に、あるいは前記ユーザ端末に構築されたユーザ情報管理装置におけるユーザ情報管理方法であって、前記ユーザ端末を利用する複数のユーザに関するユーザ情報をセキュリティレベルと関連づけて保持するための記憶ステップと、前記ユーザが前記サーバにアクセスして、所定のアプリケーションを利用しようとしたとき、前記ユーザを識別する識別ステップと、前記ユーザが前記サーバにアクセスしたとき、あらかじめ定められた複数の認証レベルのいずれの認証レベルであるかを判定するレベル判定ステップと、前記記憶ステップで保持された前記ユーザ情報の中で、前記判定されたレベルに対応する前記セキュリティレベル及びそれ以下のセキュリティレベルのユーザ情報のみを前記ユーザ端末及び／又は他の装置に対して送信可能とする送信制御ステップと、前記送信制御ステップにより送信可能とされた後、所定時間の経過及び／又は所定動作の実行後に、あるいは前記ユーザからの所定の指示に応じて前記送信可能

とされたユーザ情報を送信不可能な状態とする送信禁止ステップとを、有するユーザ情報管理方法が提供される。

また本発明によれば、ユーザ端末と双方向通信が可能なサーバ上に、あるいは前記ユーザ端末に構築されたユーザ情報管理装置におけるユーザ情報管理方法を実行するための制御プログラムがコンピュータが読み取り可能な状態で記録された記録媒体であって、前記ユーザ端末を利用する複数のユーザに関するユーザ情報をセキュリティレベルと関連づけて保持するための記憶ステップと、前記ユーザが前記サーバにアクセスして、所定のアプリケーションを利用しようとしたとき、前記ユーザを識別する識別ステップと、前記ユーザが前記サーバにアクセスしたとき、あらかじめ定められた複数の認証レベルのいずれの認証レベルであるかを判定するレベル判定ステップと、前記記憶ステップで保持された前記ユーザ情報の中で、前記判定されたレベルに対応する前記セキュリティレベル及びそれ以下のセキュリティレベルのユーザ情報のみを前記ユーザ端末及び／又は他の装置に対して送信可能とする送信制御ステップと、前記送信制御ステップにより送信可能とされた後、所定時間の経過及び／又は所定動作の実行後に、あるいは前記ユーザからの所定の指示に応じて前記送信可能とされたユーザ情報を送信不可能な状態とする送信禁止ステップとを、有するユーザ情報管理方法を実行するための制御プログラムがコンピュータが読み取り可能な状態で記録された記録媒体が提供される。

なお、前記判定されたレベルに対応する前記セキュリティレベルより低いセキュリティレベルのユーザ情報のみを前記ユーザ端末及び／又は他の装置に対して送信可能とすることは本発明の好ましい態様である。

また、前記ユーザ識別のために、前記ユーザ端末において前記ユーザが入力するパスワード、あるいは前記ユーザ端末が読み取るＩＣカード

情報、磁気カード情報、前記ユーザの指紋、声紋、虹彩紋のうちいずれか１つ以上を用いることは本発明の好ましい態様である。

また、前記レベル判定のために、前記ユーザがユーザ識別のために用いたあらかじめ定められた手法を判断することによりレベルを判定することは本発明の好ましい態様である。

また、前記ユーザ端末において前記ユーザが操作する入力装置からの所定指示に基づき前記ユーザを判断し、この場合前記レベル判定において最も低い認証レベルであると判定することは本発明の好ましい態様である。

また、前記送信制御のために、前記ユーザの現在の認証レベルが求められたデータ取得に必要な認証レベルより低い場合は、前記必要な認証レベルに引き上げるため前記ユーザに対して必要な行動をとるよう指示することは本発明の好ましい態様である。

また、前記送信制御のために、前記ユーザ情報に固有のセキュリティレベルを定義し、前記セキュリティレベル毎に前記ユーザ情報を管理することは本発明の好ましい態様である。

また、前記ユーザ端末を利用する複数のユーザに共通の情報をもグループデータとしてセキュリティレベルと関連づけて保持することは本発明の好ましい態様である。

また、要求されたデータの集合に対して、その事象となる確率とデータ間の距離からＩＤとなる指数を求め、その値を用いてセキュリティを再チェックすることは本発明の好ましい態様である。

また、前記複数のユーザ端末をあらかじめ複数のセキュリティ区分に分類しておき、セキュリティ区分判定により、アクセスしてきた前記ユーザ端末のセキュリティ区分毎にアクセス制限を加えることは本発明の好ましい態様である。

また、前記ユーザ端末の前記セキュリティ区分を当該ユーザ端末の登録ユーザ数で決定することは本発明の好ましい態様である。

また、前記セキュリティ区分中、所定の区分に該当するときは、認証レベルが低いものに移行したときに、前記認証レベルが低いものに移行する以前に前記サーバから前記ユーザ端末に伝送したデータを削除することは本発明の好ましい態様である。

また、前記セキュリティ区分中、所定の区分に該当するときは、前記ユーザ端末から前記サーバの所定作業エリアに対して前記ユーザ端末から入力されたデータを自動的及び／又は定期的に伝送することは本発明の好ましい態様である。

また、データを要求する側のユーザ情報利用基準をあらかじめ格納しておき、またデータを提供する側のユーザ情報提供条件をあらかじめ格納しておき、前記ユーザ情報利用基準と前記ユーザ情報提供条件とを比較し、比較結果により送信制御をする際に、データ中に前記ユーザ判定手段にて判断されたユーザ以外のユーザ情報が含まれている場合には、当該ユーザの前記ユーザ情報提供条件を求め、前記ユーザ情報利用基準との比較を行うことによって送信するか否かの判断をすることは本発明の好ましい態様である。

また、ユーザ情報管理装置が、データへのアクセスをアクセス受付部で受け付け、その受け付けられたアクセスのデータに対するアクセス権限をアクセス権判断部で判断し、更に、アクセス受付部で受け付けられたアクセスのデータに対するアクセス権限をアクセス管理部で変更することは本発明の好ましい態様である。

また、アクセス権判断部でのアクセス権限の有無は、データとアクセス権限とを関連付けたアクセス権限テーブルに基づいて判断されることは本発明の好ましい態様である。

また、アクセス権判断部でのアクセス権限の有無は、データに記述されているアクセス権限に基づいて判断されることは本発明の好ましい態様である。

また、アクセス管理部は、アクセス権限変更情報出力手段を有し、変更されたアクセス権限を示す情報を出力することは本発明の好ましい態様である。

また、アクセス判断部は、アクセス権限変更情報取得手段を有し、アクセス権限変更情報出力手段からの情報を取得することは本発明の好ましい態様である。

また、アクセス受付部が機器からアクセスを受け付け、アクセス権限変更情報出力手段が、その機器へ情報を送信することは本発明の好ましい態様である。

また、アクセス権限変更条件取得部を備え、アクセス権限の変更のための条件を取得することは本発明の好ましい態様である。

また、アクセス管理部におけるアクセス権限の変更は、アクセスすることができるデータの範囲であることは本発明の好ましい態様である。

また、アクセス管理部におけるアクセスされるデータに関連付けられている所有者の変更であることは本発明の好ましい態様である。

また、アクセス管理部は、アクセスの変更による処理の終了後に元のアクセス権限に復帰することは本発明の好ましい態様である。

また、アクセス受付部でのアクセスが権限の無いものであると判断された場合に、アクセス権限の取得を要求する認証取得部を有することは本発明の好ましい態様である。

また、アクセス権限変更条件取得部が取得する条件は、アクセス放置時間、データアクセス回数、アクセス者からの指示、オペレーティングシステムからの指示、アプリケーションプログラムからの指示、アクセ

ス開始後経過時間、時刻情報、アクセス拒絶回数のいずれか一または二以上の組み合わせであることは本発明の好ましい態様である。

また、ユーザ情報管理プログラムが、計算機に対してアクセス受付ステップによってデータへのアクセスを受付させ、アクセス権判断ステップによってアクセス権限の有無を判断させ、アクセス管理ステップによりアクセス受付ステップによって受け付けられたアクセスのデータに対するアクセス権限を変更させることは本発明の好ましい態様である。

また、アクセス管理ステップにおいて、変更されたアクセス権限を示す情報を出力させることは本発明の好ましい態様である。

また、アクセス権限変更情報取得ステップにおいてアクセス権限の変更のための条件を取得させることは、本発明の好ましい態様である。

図面の簡単な説明

図１は、本発明に係るユーザ情報管理装置が適用される通信システムの概略構成例を示す模式図である。

図２は、本発明に係るユーザ情報管理装置の第１実施の形態の模式的ブロック図である。

図３は、本発明における認証レベルの概念を説明するための模式図である。

図４は、本発明に係るユーザ情報管理装置の第２実施の形態を説明するための模式図である。

図５は、本発明に係るユーザ情報管理装置の第２実施の形態の動作を説明するための模式図である。

図６は、本発明に係るユーザ情報管理装置の第４実施の形態の模式図である。

図７は、本発明の各実施の形態において、データ固有セキュリティレ

ベル記憶手段における、記憶される記述内容（定義）の例を示す図である。

図８は、本発明の各実施の形態において、個人別データの例を示す図である。

図９は、本発明の各実施の形態において、レベル１のインスタンスが生成したデータの例を示す図である。

図１０は、本発明の各実施の形態において、レベル２のインスタンスが生成したデータの例を示す図である。

図１１は、本発明の各実施の形態において、レベル３のインスタンスが生成したデータの例を示す図である。

図１２は、本発明の各実施の形態において、データ固有セキュリティレベル記憶手段における、記憶される記述内容（定義）の他の例を示す図である。

図１３は、図１の一部を含むものであって、ＥＣサイトにインターネットを経由してアクセスしている場合の模式図である。

図１４は、図１３の例で、ユーザ端末のディスプレーに表示される画面の内容などを示す図である。

図１５は、図１３の例で、ユーザ端末のディスプレーに表示される画面の内容などを示す図である。

図１６は、図１３の例で、ユーザ端末のディスプレーに表示される画面の内容などを示す図である。

図１７は、図１３の例で、ユーザ端末のディスプレーに表示される画面の内容などを示す図である。

図１８は、本発明に係るユーザ情報管理装置の第９実施の形態の模式的ブロック図である。

図１９は、本発明に係るユーザ情報管理装置の第９実施の形態のアク

セス管理部がアクセス権限を記憶している一例を示す図である。

図２０は、データとアクセス権限を関連付けたアクセス権限テーブルの一例を示す図である。

図２１は、アクセスレベルによりアクセスできるデータの範囲が狭くなったり広くなったりすることを説明する模式図である。

図２２は、アクセス権限がデータに記述されている状態を示す図である。

図２３は、データが所有者毎に類別され、データに所有者が記述されている状態を示す図である。

図２４は、本発明に係るユーザ情報管理装置の第９実施の形態のアクセス管理部がアクセスできるデータの所有者を保持する権限リストを記憶している状態を示す図である。

図２５は、現在のアクセス権限と必要なデータ表題に対して、どの所有者としてのアクセス権限が必要であるかを示すテーブルの一例図である。

図２６は、アクセスを受け付け、アクセス権限の有無を判断し、受け付けられたアクセスのアクセス権限を変更する処理のフローチャートである。

図２７は、受け付けられたアクセスのアクセス権限を変更する処理のフローチャートである。

図２８は、本発明に係るユーザ情報管理装置の第９実施の形態が認証取得部を備えた場合の模式的ブロック図である。

図２９は、アクセス権限を取得するための認証画面の一例図である。

図３０は、本発明に係るユーザ情報管理装置の第９実施の形態がアクセス権限変更情報出力手段を備えた場合の模式的ブロック図である。

図３１は、本発明に係るユーザ情報管理装置の第９実施の形態がアク

セス権限変更情報出力手段を備えた場合の処理のフローチャートである。

図３２は、本発明に係るユーザ情報管理装置の第９実施の形態がアクセス権限変更情報取得手段を備えた場合の模式的ブロック図である。

図３３は、本発明に係るユーザ情報管理装置の第９実施の形態がアクセス権限変更情報取得手段を備えた場合の処理のフローチャートである。

図３４は、本発明に係るユーザ情報管理装置の第９実施の形態がアクセス権限変更情報出力手段を備え、変更されたアクセス権限を示す情報を機器へ出力する場合の模式的ブロック図である。

図３５は、本発明に係るユーザ情報管理装置の第９実施の形態がアクセス権限変更条件取得部を備えた場合の模式的ブロック図である。

発明を実施するための最良の形態

以下、図面を参照して本発明の好ましい実施の形態について説明する。図１は本発明に係るユーザ情報管理装置の好ましい実施の形態（以下第１実施の形態という）の模式図である。図１において、情報家電サーバ１０は、複数の利用者の家庭１４、１６にある複数のユーザ端末１４ａ、１６ａ、１６ｂとデジタル通信回線１２ａ、１２ｂ、１２ｃ（あるいは公衆回線）を介して接続されているものとする。各端末１４ａ、１６ａ、１６ｂはパソコンであっても、双方向通信の可能なデジタルテレビジョン（ＴＶ）であってもよい。ここではかかるデジタルＴＶが用いられているものとする。

情報家電サーバ１０は記憶手段２０を有し、ここにはユーザ情報が保持されるものとする。また、家庭１４、１６のユーザ端末１４ａ、１６ａ、１６ｂにもそれぞれ、記憶手段１８が備えられているものとする。ここでは、簡略のため、ユーザ端末１４ａ、１６ｂに備えられている記憶手段１８、２２のみが示されているものとする。これらのユーザ端末

１４ａ、１６ａ、１６ｂは実質的に同一の構成で、同一の機能を有するので、以下の説明ではユーザ端末１６ｂとサーバ１０との関係で説明する。

ユーザ端末１６ｂは、情報家電サーバ１０を介して双方向通信を行うものであり、情報家電サーバ１０はインターネットのサービスプロバイダのようにインターネット接続機能を有し、ユーザ端末１６ｂは情報家電サーバ１０を介してインターネット１３にアクセスする構成となっている。なお、図１の例では、情報家電サーバ１０とユーザ端末１６ｂの双方にユーザ情報を保持、管理するための記憶手段２０、２２が設けられているが、これらは、一方のみに存在してもよいものである。ユーザ情報としては、ユーザの氏名、住所、年齢、生年月日、性別、ブックマーク、履歴、クッキー（cookie)、クレジットカードの番号や有効期限、既往症などあらゆるものを含むことができる。なお、ユーザ情報あるいは個人情報という用語は、本明細書では、個人自体を示す情報のみならず、当該個人が操作したユーザ端末１６ｂの操作履歴などが含まれるので、過去にアクセスしたインターネットのWebサイトを示す情報などが含まれる。情報家電サーバ１０には以下に説明するユーザ情報管理装置が構築されている。

図２は、情報家電サーバ１０に構築されているユーザ情報管理装置２４の全体構成を示す模式的ブロック図である。今、ユーザ端末１６ｂが任意のアプリケーション２６を用いて情報家電サーバ１０にアクセスしているものとする。ユーザ情報管理装置２４は、ユーザ判定手段２８、レベル判定手段３０、送信制御手段３２、データ毎レベル調査手段３４、データ固有セキュリティレベル記憶手段３６、レベル毎データアクセスオブジェクト３８とを有している。なお、レベル毎データアクセスオブジェクト３８は、レベル毎にレベル毎データ記憶部４０－１～４０－３、

認証開始手段／ユーザ識別手段４２－１～４２－３、送信禁止手段４４－１、４４－２を有している。

各ブロックの機能は次のようなものである。

＃データ固有セキュリティレベル記憶手段３６

利用する複数のユーザに関連するユーザ情報をセキュリティレベルと関連付けて保持する記憶手段

＃レベル毎データ記憶手段４０－１～４０－３

データ固有セキュリティレベル記憶手段により得られ、特定ユーザが特定セキュリティレベルにおいてアクセスできるデータを保持する記憶手段であり、指定したセキュリティレベル及びそれ以下のセキュリティのユーザ情報にアクセスすることができる

＃ユーザ判定手段２８

ユーザ端末の現在のユーザを判定する手段

＃レベル判定手段３０

端末の現在のユーザが、あらかじめ定められた複数の認証レベルのいずれの認証レベルであるかを判定する手段

＃送信制御手段３２

任意のアプリケーションからのユーザ情報取得要求を受けて、ユーザの現在の認証レベルに基づいてユーザ情報を取得、あるいはデータ取得に必要な認証レベルにない場合はユーザ識別手段を呼び出して認証レベルを上げることにより、ユーザ情報を取得し送信する手段

＃送信禁止手段４４－１、４４－２

複数の認証レベルの１つに応じて選択的にデータの送信を禁止する手段

＃認証開始手段／ユーザ識別手段４２－１～４２－３

複数のユーザ識別手段のうちいずれのユーザ識別手段かを記憶し、送信制御手段からの要求に応じて当該ユーザ識別手段を呼び出すことのできる手段

＃データ毎レベル調査手段３４

データ固有セキュリティレベル記憶手段により得られ、アクセスしようとするデータが、いずれのセキュリティレベルを必要とするかを求める手段

＃任意アプリケーション２６

ユーザ情報管理装置に対して、ユーザ情報を要求するアプリケーション

ユーザ判定手段２８は、ユーザ端末１６ｂでユーザが用いた認証手段から得られる情報によりユーザを特定するものである。ユーザが用いる認証手段としては、一人に１枚が交付されているＩＣカード又は磁気カードの情報や、パスワードの入力により実現される。また、ユーザの指紋や虹彩紋、顔画像などを用いて認証することも可能である。したがって、ユーザ端末１６ｂには、使用される認証手段に応じた図示省略のカードリーダや、撮像装置と、これらのインターフェイスや駆動装置が備えられる。

本発明では、ユーザ毎に複数の認証レベルが設けられ、どの認証レベルかによって、アクセスできるデータの範囲を異ならせるように管理している。すなわち、認証開始手段／ユーザ識別手段４２－１～４２－３と送信禁止手段４４－１、４４－２は、認証されたレベルでアクセスできるデータを管理している。ここで「認証開始」とは、所定のレベルで認証を開始することを意味し、「送信禁止」とは、所定のレベルでの認証を終了することを意味する。

図３は、本発明で認証レベルが３つ設けられた場合のデータスコープ

を示す模式図である。それぞれのセキュリティレベルに対し、この図を上から見た範囲のデータに対してアクセスできる。すなわち、セキュリティレベルが最も高いレベル１（Level1）では、Level1 から Level3 の全てのデータにアクセスでき、逆にセキュリティレベルが最も低いレベル３(Level3)の場合は Level3 の部分のデータにのみアクセスできる。これら３つのレベルは、上述のユーザ判定に用いられた認証手段にそれぞれ対応している。ユーザがＩＣカードを用いたときは、レベル１とされ、パスワードを入力したときは、レベル２とされ、またこれらを用いないときはレベル３とされる。認証の終了である送信禁止は、所定時間の経過（タイムアウト）により、あるいは所定の動作の実行により実行される。所定の動作としては、例えば１回のデータ取得などとすることができる。

認証レベルの高低は次のような意味を有する。すなわち、高い認証レベルでは、そのレベルとそれ以下のレベルでアクセスできるデータにアクセスすることができる。すなわち、認証レベルの高低によりアクセス可能なデータの範囲が変化するのである。最下位の認証レベルであるレベル３には、送信禁止手段はない。これはレベル３から認証を終了することはないからである。換言すれば、ユーザが判定された段階で最低でもレベル３の認証レベルとなり、１６ｂにパスワードを入力して情報家電サーバ１０で認証されるとレベル２となり、さらに１６ｂにＩＣカードを挿入して情報家電サーバ１０で認証されるとレベル３となるのであり、時間の経過などに伴い、レベル３からレベル２へ、さらにレベル１へと変化するのである。

次に１６ｂにより情報家電サーバ１０にある所定のデータにアクセスする場合について説明する。

1.あるデータにアクセスする場合は、ユーザ判定手段２８でアクセスす

るユーザを判定し、次いでレベル判定手段３０で、その認証レベルを調べ、そのレベルに対応したレベル毎データアクセスオブジェクト３８をアクティブにする。図２では、３つのレベルのそれぞれについて、レベル毎データ記憶手段、認証開始手段／ユーザ識別手段、送信禁止手段（第１レベルと第２レベルのみ）からなるデータアクセスオブジェクトが示されている。

2. レベル毎データ記憶部４０－１～４０－３は、その値を取得できれば値を返す。取得できない場合は、その旨のエラーコードを返す。

3. 送信制御手段３２は上記２においてエラーコードが返ればデータ毎レベル調査手段３４において、そのデータアクセスに必要なレベルを調べる。

4. 上記３で求めたレベルのレベル毎データアクセスオブジェクトがアクティブでなければアクティブとし、再度データを要求する。また、アクティブにしたレベル毎データアクセスオブジェクトの認証開始手段／ユーザ識別手段４２－１～４２－３により、認証を開始する。認証開始に成功すれば、レベル毎データ記憶部４０－１～４０－３へデータ要求をする。

5. 既にアクティブとなっているレベル毎データアクセスオブジェクト３８を使用する場合は送信禁止手段４４－１、４４－２により、認証された状態をチェックする。送信禁止手段４４－１、４４－２はタイマーやセッション終了などの定義された手段により認証終了となったかどうかを判断する。

認証開始手段においてユーザ変更機能をもたせることにより、”子供のレベル３”状態から”レベル１”データにアクセスしようとしたときに、”子供”→”母”というようにユーザまで変更することも可能である。このように、レベルアップ時は認証が必要であり、ここでユーザを変更で

きる。また自動的にレベルダウンする。このときレベルによってデータスコープが変わるのである。

上記構成の効果はつぎのようなものである。

●１度認証すると、それ以下の認証レベルのデータには全てアクセスでき、アプリケーションやデータごとに個別に認証する必要がない。

●タイムアウトなどにより自動的に認証レベルが下がっても、同じユーザとしての権限は失わない。最低レベルでのユーザデータへのアクセスができる(通常はログアウトするなど､そのユーザとしての権限を失う)。

＜第２実施の形態＞

上記第１実施の形態の「レベル毎データ記憶部」において、ある特定のユーザでデータにアクセスする場合、図４に示すように個人のデータに加えてそのユーザが属するグループのデータもアクセスすることができる。さらに、それぞれのデータに対し、個人データか、グループデータかを定義できる。図５は、母がレベル２でアクセスしたときのデータスコープの例を示している。

例えば履歴など無意識のうちに蓄積されるデータを家族の最も低いレベルのデータとすることにより、ログインがタイムアウトになったまま放置されて不特定多数のユーザが閲覧しているような状態で、ユーザ切替を敢えてする必要はなく、(個人データにアクセスするときに初めてユーザ認証などを求められる）スムーズな作業ができる。また、家族共通のデータ（住所など）をグループデータとすることにより、共通の値を共有できる。データごとに個人データか、グループデータかを定義できることにより、ユーザ識別をきちんと行う家族、ほとんど行わない家族など、使い方に合わせて定義することができる。

＜第３実施の形態＞

第１実施の形態の「データ固有セキュリティレベル記憶手段」３６に

おいて、それぞれのデータ毎のセキュリティレベルを求めることができる。例：クレジットカード番号にアクセスできるのはセキュリティレベル１、年齢や性別にアクセスできるのはセキュリティレベル２など。「年齢」、「性別」を単体で提供しても、ＩＤとはならないが、一緒にデータを渡すと個人を特定できる確率が高まってしまう。すなわち、複数のデータにより、「個人を特定できる」こととなるので、高いセキュリティレベルを必要とするのである。

第３実施の形態では、要求されたデータの集合に対して、その事象となる確率とデータ間の距離からＩＤとなる指数を求め、その値を用いてセキュリティ再チェックをする。データ単体ではアクセス可能と判断されているが、集合としての再チェックをすることにより、セキュリティの高低を見極めることができるのである。

例として、つぎのようなものがある。

単体での ID となる指数=1-確率　(例えば、「性別＝女」となる確率は 0.5)

ペアで利用したときのＩＤとなる指数＝1-確率 a×（１－距離 ab×（１－確率 b)

)

確率 a≦確率 b

距離ａｂ：データａとデータｂとの距離であり、相関で求められる

年齢と性別⇒距離は遠い

年齢と収入⇒距離は近い

同様にして、複数共用したときのＩＤとなる指数＝1-確率 a×（１－距離 ab×

（１－確率 b)) ×…×（１－距離 yz×（１－確率 z))

確率 a≦確率 b≦…≦確率 z

ここで「その事象となる確率」はデータの値より変化するが、値に関係なくデータに共通な平均確率などを用いてもよい（処理速度向上のため）。複数データを渡す渡し方は、同時でもよいし、異なるタイミングでもよい（ただし、アクセス元を同定する機能が必要となる）。

＜第４実施の形態＞

第１実施の形態に対して、図６に示すようにユーザ情報管理装置２４Ａ内には、「レベル判定手段」３０に加え、「セキュリティ区分判定部」４６と、「データ固有セキュリティ区分定義手段」４８を備え、セキュリティ区分ごとにアクセス制限を加えることができる。データ固有セキュリティ区分定義手段４８は、データ毎のセキュリティ区分を記述したものであり、判定されたセキュリティ区分と、要求されたデータのセキュリティ区分とを比較して送信可能か否かを判断するために用いられる。

例として、つぎのようなものがある。

セキュリティ区分：個人の端末／居間の端末／ホテルの端末など

ログインなどのときに、履歴、ブックマーク、クッキー（cookie）、個人情報などをサーバから端末に伝送する際、端末のセキュリティ区分により伝送するデータの範囲を変えることができる。

＜第５実施の形態＞

第４実施の形態においてユーザ端末のセキュリティ区分を登録ユーザ数で決定する。すなわち、登録ユーザが登録されていなければ、ホテルの端末のように不特定多数と判断する。

＜第６実施の形態＞

第４実施の形態においてセキュリティ区分によってはタイムアウトやログアウトなどによりセキュリティレベルが低いものに変更されたときに、ユーザ端末に伝送したデータを削除する。すなわち、所定のセキュリティ区分のときは、セキュリティレベルが低下したときは先にセキュ

リティレベルが高い状態で伝送したデータを自動的に削除して、かかるデータの流出や悪用を防止するものである。

＜第７実施の形態＞

第１実施の形態においてセキュリティレベルによっては定期的、自動的に端末からサーバの個人情報作業スペースへデータを伝送する。突然電源を切られたら、そこから作業中データを復旧することができる。また、セキュリティレベルによってはこのバックアップ処理を行なわないことで、通常の処理は軽く、重要なデータのみを復旧可能とできる。

＜第８実施の形態＞

Ｐ３Ｐプロトコルを用いることにより、Ｗｅｂサイトに個人情報を渡す際に、ユーザのポリシー（プリファレンス）とＷｅｂサイトのポリシーを比較して、セキュリティチェックを行なうことができる（「Ｐ３Ｐプロトコル」は、例えば「日経インターネットテクノロジー」２０００年１月号ｐｐ１２５－１３６に示されている）。しかし、ユーザが他人のプライバシーを侵害することに関してのチェックのしくみはない。第８実施の形態では、情報家電サーバのように、複数人の個人情報を管理するシステムにおいて、他人の個人情報に関する場合はまずその人のデータを検索し、ポリシーをチェックして個人情報を伝送してよいかどうかを判断する。伝送してよいと判断された場合には、そのデータを取得できる。

具体的には、図２中の送信制御手段３２の外部にユーザ情報利用基準記憶手段と、個人毎ユーザ情報提供条件記憶手段と、条件比較部と、該当ユーザ検索手段を設けるのである。ここで、ユーザ情報利用基準記憶手段は、ユーザ情報を要求する側が受け取ったデータをどのように利用するかという基準を記憶する手段で、あらかじめ管理者が登録しておき、運用時にデータを要求する任意のアプリケーションがデータを要求する

と、この基準が読み出される。データの利用方法の例としては、統計のため、開発のため、個人識別のため、個人識別以外のためなどが挙げられる。個人毎ユーザ情報提供条件記憶手段は、ユーザ情報を提供する側の提供条件を記憶する手段で、個人毎に条件を設定しておくことができる条件はユーザによりあらかじめ登録され、運用時にデータを要求する任意のアプリケーションがデータを要求すると、この条件が読み出される。条件比較手段は、上記それぞれ読み出されたユーザ情報利用基準と個人毎ユーザ情報提供条件とを比較することによりユーザ情報を提供してよいかどうかの判断をする手段である。

この判断結果が送信制御手段３２に与えられる。該当ユーザ検索手段は、送信制御手段３２からのデータ要求を示す信号に応じて要求されたユーザ情報がどのユーザのものなのかを検索し、該当ユーザが得られた場合には、個人毎ユーザ情報提供条件記憶手段にアクセスして、そのユーザのユーザ情報提供条件を得る手段である。なお、ここでいうどのユーザのものかとは、いまユーザ端末１６ｂにアクセスしているユーザ以外のユーザのことであり、現在アクセスしているユーザが自分以外のユーザの情報を求める場合は、それを示す信号、例えば "other users" などをサーバ１０のユーザ情報管理装置２４に送信し、この信号が送信制御手段３２を介して該当ユーザ検索手段に与えられるのである。この構成により、送信制御手段３２は、認証レベル毎の送信制御に加えて、ユーザ情報利用基準とユーザ情報提供条件の比較結果によりユーザ情報の送信制御を行うのである。

具体的動作例として次のようなものがある。例えば、Ｗｅｂアンケートに家族に対しての記述欄があったとする。そこで家族のそれぞれについて個人データを検索し、家族の一人一人のポリシーをチェックして、氏名、性別、年齢などをそのＷｅｂサイトに渡してよいかどうかを判断

する。渡してよい場合は結果としてそれぞれの値が得られる。

＜各実施の形態の共通事項＞

次に各実施の形態の共通の事項について更に説明する。図７は、データ固有セキュリティレベル記憶手段３６における、記憶される記述内容（定義）の例である。この例は、特定の人のデータにアクセスする場合に有効なものである。子供用データ定義／大人用データ定義といった複数の定義を用意してもよい。この記述中で、<Dynamic accessLevel=" 3" >と記載された部分は、この特定のデータがレベル３であることを示している。

図８は、データ固有セキュリティレベル記憶手段３６に同じく記憶される個人用データの例を示すものである。上記図７と図８の各データは、ユーザ端末１６ｂを購入した直後に登録すべき事項である。すなわち、ユーザ自身が情報家電サーバ１０にアクセスしてこれらを記述することもできるし、アンケート用紙に家族のデータなどを記載して情報家電サーバ１０の管理者に送付し、管理者が登録してもよい。

上記登録後、実際の使用時にユーザ端末１６ｂからデータの要求があると、データ属性定義と個人別データを解析して図９～図１１に示すようなデータを作る。両方にアクセスレベルが設定されている要素についてはユーザのアクセスレベルを優先してもよいし、レベルの高い項目を優先してもよい。図９～図１１は、それぞれレベル１～レベル３のインスタンスが生成したデータ例を示している。

次に、図１２に、データ固有セキュリティレベル記憶手段３６における、記憶される記述内容（定義）の他の例を示す。この例は、不特定多数のあるデータを一度に取り出す場合に有効なものである。データを登録する際に、セキュリティレベルで分割されたＤＢに格納する。セキュリティレベルは、それぞれのデータ定義において定められた値と、デー

タ登録の際に個別に指定された値から決定される。

＜本発明をＥＣサイトによる買い物に用いた場合の具体例＞

次に、本発明を用いてＥＣ（エレクトロニックコマース）サイトにアクセスして買い物をする場合について説明する。図１３は、図１の一部を含むものであって、ＥＣサイト５０にインターネット１３を経由してアクセスしている場合の模式図である。図１４は、ユーザ端末１６ｂのディスプレーに表示される画面の内容を示している。いま、ユーザがリモコンボタンや、画面上のユーザ指定部分を選択してユーザ端末１６ｂにアクセスしたものとすると、当該ユーザの現在のレベルはレベル３と認定される。ここで、買い物を実行しようとして、「清算する」という画面内のボタン部分をクリックすると、会員番号及びパスワードを尋ねる画面に切り替わる。すなわち、ユーザ情報管理装置２４がレベル３でアクセスしているユーザに対してレベル１へレベルアップする必要があるので、これらの情報の入力を求めるのである。

ユーザ情報管理装置２４での一連の動作はつぎのようなものとなる。FooShop.UserID 及び FooShop.UserPasswd のセキュリティレベルは１とする。

1.現在のレベル３のレベル毎データアクセスオブジェクトは既にあり、送信禁止手段４４－１、４４－２をチェックすると、レベル３のままであることが判る。

2.レベル毎データアクセスオブジェクトに FooShop.UserID 及び FooShop.UserPasswd を要求する。

3.エラーが返る。

4.データ毎レベル調査部により FooShop.UserID 及び FooShop.UserPasswd のセキュリティレベルを求めると、レベル１であることがわかる。

5.レベル判断部はレベル１のレベル毎データアクセスオブジェクトを生成する。

6.認証開始手段４２－１に設定されている認証手段を呼び出す。

7.図１５の画面がユーザ端末１６ｂのディスプレーに表示される。

8.認証が正常終了したら、FooShop.UserID 及び FooShop.UserPasswd を要求すると、値が得られる。

9.元のコードに得られた値を補完する。

<INPUT TYPE="text" NAME="FooShop.UserID" value=" 11223344"

<INPUT TYPE=" password " NAME="FooShop.UserPasswd " value=" 55667788" >

10.値を補完した文書をユーザに送る。

この結果、ユーザ端末１６ｂのディスプレーには図１４の下方に示すような画面が表示される。ユーザがＯＫを押すと、ＥＣサーバは図１６に示す画面を返す。次いでユーザ情報管理装置２４は、次のようにユーザ情報を求める。

User.Name, User.Postal.Postalcode, User. Postal.Formatted, User. Telecom.Telephone のセキュリティレベルは２とする。

1.現在のレベル１のレベル毎データアクセスオブジェクトの送信禁止手段４４－１をチェックすると、レベル１は無効になっていることがわかる。

2.レベル２のレベル毎データアクセスオブジェクトを生成する。

3.レベル毎データアクセスオブジェクトに User.Name, User.Postal.Postalcode, User. Postal.Formatted, User. Telecom.Telephone を要求する。

4.元のコードに得られた値を補完する。

<INPUT TYPE="text" NAME="User.Name" value=" 山田太郎" >

<INPUT TYPE="text" NAME="User.Postal.Postalcode" value="123-0000" >

<INPUT TYPE="text" NAME="User. Postal.Formatted" value="東京都 …" >

<INPUT TYPE="text" NAME="User. Telecom.Telephone" value="03-1234-5678" >

5.値を補完した文書をユーザに送る。

この結果、ユーザ端末１６ｂのディスプレーには、図１７に示すような画面が表示される。

上記各実施の形態などでは、ユーザ情報管理装置２４が情報家電サーバ１０上に構築されているものとして説明したが、ユーザ情報管理装置２４は、ユーザ端末１４ａ、１６ａ、１６ｂに構築してもよい。この場合も、上記説明と同様の動作を行うことができる。

＜第９実施の形態＞

図１８は、第９実施の形態に関するユーザ情報管理装置の機能ブロック図である。ユーザ情報管理装置１８０は、アクセス受付部１８２とアクセス権判断部１８４とアクセス管理部１８５より構成される。

アクセス受付部１８２は、データ１８３へのアクセス１８１を受け付ける。データ１８３は図１８に示すようにユーザ管理装置１８０の内部にあってもよいし、外部にあってもよい。ここに、アクセス受付部１８２が受け付ける「アクセス」とは、データを特定して、そのデータに対して処理を施す指令あるいは命令である。例えば、データを読み出すこと、書き込むこと、削除すること、複製を作ること、内容を変更すること、あるいは、新しくデータを追加することが例として挙げられる。

アクセス権判断部１８４は、アクセス受付部１８２で受け付けたアクセスのデータに対するアクセス権限の有無を判断する。すなわち、アク

セス受付部１８２にアクセスを受け付けさせた主体のアクセス権限、あるいは、ユーザ情報管理装置１８０自体のアクセス権限と、アクセス１８１によって特定されるデータのアクセス権限とを比較し、アクセス１８１によるデータへのアクセスが許されるかどうかを判断する。

アクセス管理部１８５は、アクセス受付部１８２で受け付けたアクセス１８１のデータに対するアクセス権限の変更を行う。「アクセス受付部１８２で受け付けたアクセス１８１のデータに対するアクセス権限」とは、アクセス受付部１８２で受け付けたアクセス１８１によるデータへのアクセスが権限のあるものかどうかをアクセス権判断部１８４で判断する際にユーザ情報管理装置１８０に記憶されているアクセス権限のことである。アクセス管理部１８５は、ユーザ情報管理装置１８０に記憶されているアクセス権限を変更する。先述のようにアクセス権判断部１８４がアクセス権限の有無を判断する場合には、アクセス受付部１８２にアクセスを受け付けさせた主体のアクセス権限とアクセス１８１によって特定されるデータのアクセス権限とを比較する場合と、ユーザ情報管理装置１８０自体のアクセス権限とアクセス１８１によって特定されるデータのアクセス権限とを比較する場合とがある。したがって、前者の場合には、アクセス管理部１８５はアクセス受付部１８２にアクセスを受け付けさせた主体のアクセス権限を変更する。また、後者の場合には、アクセス管理部１８５はユーザ情報管理装置１８０自体のアクセス権限を変更する。

アクセス管理部１８５がアクセス権限の変更を行うためには、変更を行うアクセス権限が記憶されている必要があるが、一つの方法として、図１９に示すようにアクセス管理部１８５の中にアクセス権限を記憶しておき、この記憶されたアクセス権限を変更する方法がある。以下では、アクセス権限がアクセス管理部１８５の内部に記憶されていると仮定し

て記述するが、アクセス権限がアクセス管理部１８５の外部に記憶されていている場合に対しても以下の説明は適用可能である。図１９では、アクセス権限は「アクセスレベル」として記憶されている。アクセス権限がアクセスレベルとして記憶されている場合には、アクセスされるデータにアクセスするのに必要なアクセスレベルが付されており、アクセス管理部１８５に記憶されているアクセスレベルがデータに付されたアクセスレベル以上であればアクセス権限が有るとアクセス権判断部１８４によって判断される。

図２０は、データとアクセス権限とを関連付けたアクセス権限テーブルの一例を示している。このテーブルの各行が、どのデータにアクセスを行う場合に、どれだけのアクセスレベルがアクセス管理部１８５によって記憶されていなければならないかを示している。例えば、図２０のテーブルの第一行は、データＡに対しては必要アクセスレベルが１であることを示している。従って、データＡにアクセスするには、アクセス管理部１８５にはアクセスレベルが１以上でなければならないことになる。なお、図３においては、レベル１を最もセキュリティレベルが高いとしたが、本実施の形態においては、説明の都合上、アクセスレベルが１であるものが一番低いアクセスレベルにあり、アクセスレベルの数字が高くなるに従ってアクセスに必要とされるアクセスレベルが高くなるとしている。

このように、データに付されたアクセスレベル以上のアクセスレベルがアクセス管理部１８５に記憶されていなければいけないということは、アクセス管理部１８５にアクセスレベルが１が記憶されている場合よりも２が記憶されている場合の方がアクセスできるデータの範囲は広くなり、更に３が記憶されている場合の方が２が記憶されている場合よりもアクセスできるデータの範囲は広くなり、これを模式的に図で示すと図

２１のようにアクセスレベルが高いものがアクセスレベルが低いものを包含する関係になる。

なお、記憶されているアクセスレベルが高ければ、それより低いアクセス権限を必要とするデータにアクセスできるとし、図２１のようなアクセスレベルが高いものがアクセスレベルを低いものを包含する模式図を書いたが、記憶されているアクセスレベルと、アクセスされるデータのアクセスレベルが等しい時に限り、データにアクセスできるようにすることもできる。この場合、高いアクセスレベルが記憶されていても、低いアクセスレベルを必要とするデータにアクセスすることができないことになり、結果として、無制限にデータがアクセスできてしまうことを防止することができるようになる。

図２０は、アクセスされるデータにアクセス権限であるアクセスレベルをテーブルによって付した例であるが、データそのものにアクセス権限を記述する場合もあり、アクセス権判断部１８４は、データそのものに記述されたアクセス権限に基づいてアクセス権限の有無を判断する。図２２は、データそのものにアクセス権限が記述されている例を示している。図２２では、データＡは年収を表すデータであり、このような年収を表すデータは特にプライバシーに関わるデータであるので、３という高いアクセスレベルが記述されている。また、データＢは、住所を表すデータであるが、年収に比べると機密性は低くなるので、年収のアクセスレベルより低い１というアクセスレベルが記述されている。データＣは名前というデータであるが、これは住所よりは機密性が高く、年収よりは機密性が低いので、アクセスレベルが２に設定されている。

また、アクセスされるデータは所有者ごとに類別されるようにしてもよい。図２３は、そのような例であり、データＡの所有者は甲、データＢの所有者が乙、データＣの所有者が丙であると各データに記述されて

いることを図示している。もちろん、データの所有者をデータに記述せずに、図２０のようにデータとその所有者とを関連付けるテーブルを用いることにしてもよい。

このようにアクセスされるデータが所有者ごとに類別される場合には、アクセス管理部１８５は、アクセス権限として、現在どの所有者のデータにアクセスできるかを記憶することになる。図２４はアクセス管理部１８５の中に「権限リスト」としてアクセスできるデータの所有者をリスト構造によって記憶している例であり、この例では、「丙」または「乙」が所有者になっているデータにアクセスする権限があることになる。このようにアクセス管理部１８５に権限リストが記憶されている場合には、アクセス権限の変更は、アクセスしているデータに関連付けられている別の所有者のデータへするアクセスの変更となる。すなわち、アクセスするデータに関連付けられている所有者を権限リストに追加する、あるいは、アクセスするデータに関連付けられている所有者に権限リスト全体を入れ替えることを行うことになる。

このようにアクセスされるデータが所有者ごとに類別され、アクセス権限として現在どの所有者のデータにアクセスできるかを記憶している場合には、あるデータにアクセスする必要が発生した時に、現在のアクセス権限とアクセスする必要となったデータから、どのようなアクセス権限を得るべきかを知ることができる。図２５は、現在のアクセス権限とアクセスする必要となったデータから、どのようなアクセス権限を得るべきかを示すテーブルの一例であり、例えば、そのテーブルの第一行は、(丙、クレジットカード番号、甲)の３つのデータから成っているが、これは、現在のアクセス権限が丙であり、必要なデータがクレジットカード番号である場合に、クレジットカード番号のデータをアクセスするには、甲のアクセス権限が必要であることを示している。したがって、

現在、丙のアクセス権限がアクセス管理部１８５に記憶されている場合に、クレジットカード番号が必要になり、クレジットカード番号をアクセスしようとすると、甲のアクセス権限が必要となり、もし、甲のアクセス権限がアクセス管理部１８５に記憶されていない場合には、甲のアクセス権限を獲得する処理が起動されるようにすることができる。

なお、アクセス権限としてアクセスレベルを用いる場合と所有者を用いる場合とは排斥しあう関係にはなく、この２つの場合を組み合わせることが可能である。例えば、データを所有者ごとに類別し、同じ所有者に類別されたデータにアクセスレベルを個別に付することが可能である。また、逆に、データをアクセスレベルごとに類別し、同じアクセスレベルに類別したデータに所有者を割り当てておくこともできる。この場合、アクセス権限の有無の判断は、データのアクセスレベルとアクセス管理部１８５に記憶されているアクセスレベルの比較と、データの所有者とアクセス管理部１８５に記憶されている所有者とを比較することになる。

図２６と図２７とは、このようにアクセス権限としてアクセスレベルと所有者とを用いる場合に、データに対するアクセスを受け付け、アクセス権限の有無を判断し、また、アクセス権限が無いと判断された場合に、アクセス権限を調整する処理を説明するフローチャートである。

ステップＳ２６１において、データへのアクセスを受け付ける。

ステップＳ２６２において、アクセス権限を得る。すなわち、アクセス管理部１８５で記憶されているアクセス権限を得る。

ステップＳ２６３において、データにアクセスするのに必要なアクセス権限とステップＳ２６２で得られたアクセス権限を比較し、データに対するアクセス権限があるかどうか判断し、アクセス権限があればステップＳ２６４へ移行し、データへのアクセスを許可する。

ステップＳ２６３において、データに対するアクセス権限が無いと判

断されるとステップＳ２６５へ移行し、必要に応じてアクセス権限を変更する。

必要に応じてアクセス権限を変更する処理について説明したフローチャートが図２７に示されている。

ステップＳ２７１において、データに対するアクセス権限が低すぎるかどうかを判断する。すなわち、アクセス管理部１８５に記憶されているアクセスレベルが、アクセスするデータのアクセスレベルより低いかどうかを判断する。もし、低いと判断された場合には、ステップＳ２７２へ移行し、アクセス権限であるアクセスレベルを高くする処理を行う。例えば、アクセスレベルを上げるための認証を行う。

ステップＳ２７１においてデータに対するアクセス権限が低すぎないと判断された場合には、ステップＳ２７３へ移行し、データに対するアクセス権限が高すぎるかどうかを判断する。すなわち、アクセス管理部１８５に記憶されているアクセスレベルが、データをアクセスするのに必要なアクセスレベルより高いために、アクセスができない場合であるかどうかを判断する。もし、そうならば、ステップＳ２７４へ移行し、アクセスレベルであるアクセス権限を低くする。

ステップＳ２７３において、データに対するアクセス権限が高すぎないと判断された場合、すなわち、記憶されているアクセスレベルとアクセスされるデータのアクセス権限のアクセスレベルが等しい場合には、記憶されている所有者とデータの所有者が異なるので、ステップＳ２７５へ移行し、別のアクセス権限を得る。すなわち、別の所有者としてのアクセス権限を得ることになる。

このような処理により、データにアクセスを行い、アクセス権限の理由によりデータにアクセスができなかった場合に、別のアクセス権限を獲得するなどの調整作業を行い、再びデータへのアクセスを試みるので、

アクセス権限の理由でエラーが生じて処理が中断することがなくなる。

なお、図２７においては、アクセス管理部１８５に記憶されているアクセスレベルがデータをアクセスするのに必要なアクセスレベルと同じでないとアクセス権限が無いと判断されることを仮定したが、アクセス管理部１８５に記憶されているアクセスレベルがデータをアクセスするのに必要なアクセスレベル以上であればアクセス権が有ると判断される場合には、ステップＳ２７３、ステップＳ２７４は不要であり、ステップＳ２７１でＮに分岐した場合には、ステップＳ２７５へ移行すればよい。また、図２７においては、アクセスレベルと所有者との両方でアクセス権限の有無を判断したが、アクセスレベルのみで判断する場合や所有者のみで判断する場合に図２７のフローチャートが適合できるように変形することは容易である。

また、ステップＳ２７２、ステップＳ２７４、ステップＳ２７５において、アクセス権限を変更する際に、変更前のアクセス権限を記憶しておき、その後にデータのアクセスを試みた後で、ステップＳ２７２、ステップＳ２７４、ステップＳ２７５において変更される前のアクセス権限に戻るようにすることもできる。このようにすることにより、一時的に高いアクセス権限が得られても元のアクセス権限に戻ることが保障されるので、高いアクセス権限のまま作業が行われ、予想外のデータが読み出されたり、データが破壊されたりすることを防止することができる。

ステップＳ２７２、ステップＳ２７４、ステップＳ２７５において、アクセス権限を変更するために、図２８に示すように、ユーザ情報管理装置１８０は認証取得部２８１を備えていてもよい。すなわち、認証取得部２８１は、アクセス受け付け部１８２でのアクセスが権限のないものであるとアクセス権判断部１８４で判断された場合に、アクセス権限の取得を要求する。例えば、ユーザ情報管理装置１８０にディスプレー

とキーボードとが接続されている場合には、認証取得部２８１はディスプレーに図２９にようなユーザ名とパスワードを要求する画面を表示し、ユーザがキーボードを用いて入力したユーザ名とパスワードが正しいかどうかを判断し、正しいと判断した場合には、アクセス管理部に対してアクセス権限を変更する要求をする。あるいは、ユーザ情報管理装置１８０にＩＣカードを受け付ける部分があれば、認証取得部２８１はＩＣカードによる認証を行い、アクセス管理部に対してアクセス権限を変更する要求をするようにしてもよい。また、ユーザ情報管理装置１８０に認証を行うためのディスプレーとキーボードとが直接接続されている必要はなく、ユーザ情報管理装置１８０に端末装置が接続された状態であってもよい。この場合には、認証取得部２８１は端末装置に認証取得要求を送信し、端末装置が認証取得要求に応じてパスワードやＩＣカードなどによる認証を行い、その結果を認証取得部２８１へ送信することになる。また、端末装置が認証取得部２８１の動作とは独立に認証を行い、その認証の結果をユーザ情報管理装置１８０のアクセス受付部１８２へ受け付けさせるアクセス１８１とともに送信し、認証取得部２８１がその認証の結果を取得するようにしてもよい。結果として、アクセス権限の変更にともなう認証は、ユーザ情報管理装置１８０が処理の主体となって行うこともできるし、また、ユーザ情報管理装置１８０以外の端末装置が処理の主体となって行うこともできる。

このように、ユーザ情報管理装置１８０が認証取得部２８１を備え、図２６と図２７とに示された処理を行うことにより、アクセス権限判断部１８４でアクセスが権限のないもので判断された場合には（ステップＳ２６３）、アクセス管理部１８５がアクセス権限の変更を行うための認証を行い、その認証に成功した場合にアクセス権限の変更が行われて（ステップＳ２７２、ステップＳ２７４、ステップＳ２７５）データへのア

クセスができるようになるので、処理全体がアクセス権限の無いことにより中断されることなくスムーズにアクセス権限の変更が行われる。またアクセス権限の変更は正しく認証が行われた場合にのみ行われるので、不正なアクセスができなくなる。

また、アクセス管理部１８５は、図３０に示すようにアクセス権限変更情報出力手段３０１を備えてもよい。アクセス権限変更情報出力手段３０１は、アクセス管理部１８５がアクセス権限を変更した場合、アクセス権限変更情報を出力する。アクセス権限変更情報とは、変更されたアクセス権限を示す情報であり、例えば、アクセス権限が変更された事実のみを示したり、あるいは、アクセス権限の変更により、どのようなアクセス権限が記憶されているかを示したりする。

図３１は、ユーザ情報管理装置がアクセス権限変更情報出力手段３０１を備える場合のユーザ情報管理装置の処理のフローチャートである。

ステップＳ３０１において、アクセス権限を変更する条件が成立するまで待つ。アクセス権限を変更する条件が成立すると、ステップＳ３０２に移行し、アクセス権限を変更する。そして、ステップＳ３０３において、アクセス権限変更情報を出力する。

アクセス権限変更情報出力手段３０１がアクセス権限変更情報を出力する出力先としては、アクセス権判断部１８４が有するアクセス権限変更情報取得手段が挙げられる。すなわち、アクセス権限変更情報取得手段は、図３２に示すようにアクセス権判断部１８４の中にあり、アクセス権限変更情報出力手段３０１が出力するアクセス権限変更情報を受信する。

図３３は、アクセス権限変更情報取得手段の動作を示すフローチャートであり、ステップＳ３３１において、アクセス権限変更情報を受信するまで待つ。アクセス権限変更情報が受信されたら、ステップＳ３３２

へ移行し、保持されているアクセス権限を変更する。この場合、アクセス権限はアクセス管理部１８５のみならず、アクセス権判断部１８４にも保持されているとし、ステップＳ３３２において変更されるのはアクセス権判断部１８４に保持されているアクセス権限である。

このようにアクセス権判断部１８４がアクセス権限変更情報取得手段３２１を備えることにより、アクセス権判断部がアクセス権限を記憶することができ、アクセス管理部１８５で記憶されているアクセス権限と同期をとって変更することが可能となり、アクセス権判断部でのデータに対するアクセス権限の有無の判断の際にアクセス管理部からアクセス権限を取得する必要がなくなる。

また、図３４に示すように、アクセス受付部１８２がアクセス１８１を機器３４２から受け付ける場合に、アクセス権限変更情報出力手段３０１は、機器３４２へアクセス権限変更情報を出力するようにしてもよい。

このようにすることにより、機器３４２が現在のアクセス権限を記憶することができ、その内容がアクセス管理部１８５に記憶されているアクセス権限と同じにすることができるので、機器３４２がアクセス１８１をアクセス受付部１８２へ送信する前に、アクセス権限の判断を行うことができ、無駄なアクセス１８１の送信を防止することができる。特に、一度高いアクセス権限を獲得し、その後、アクセス管理部１８５がアクセス権限を低いものに変更した場合に、アクセス権限変更情報により、機器３４２が記憶するアクセス権限を低いものに自動的に変更することができる。したがって、機器３４２が高いアクセス権限があるものと判断して高いアクセス権限が必要なデータへアクセスを行い、アクセス権限が無いというエラーが発生して処理が中断することを防止することができる。

また、アクセス管理部１８５がアクセス権限を変更する条件を取得するために、図３５に示すようにユーザ情報管理装置１８０がアクセス権限変更条件取得部３５１を備えてもよい。アクセス権限変更条件取得部３５１は、アクセス権限の変更のための条件を取得し、その条件としては、アクセス放置時間、データアクセス回数、アクセス者からの指示、オペレーティングシステムからの指示、アプリケーションプログラムからの指示、アクセス開始後経過時間、時刻情報、アクセス拒絶回数、アクセス権限変更後経過時間の一または二以上の組み合わせが挙げられる。アクセス放置時間とは、一度アクセスが行われてからの経過時間であり、次にアクセスが受け付けられると再び０から経過時間の計測が開始される。データアクセスの回数は、アクセスを受け付けた回数、あるいは、特定のデータに対してアクセスが行われた回数である。アクセス者からの指示とは、アクセスをユーザ情報管理装置１８０へ送信する者によるアクセス権限の変更の指示である。オペレーティングシステムからの指示とは、ユーザ情報管理装置１８０を実現する計算機や、ユーザ情報管理装置１８０が接続されている計算機のオペレーティングシステムからのアクセス権限変更の指示であり、例えば、計算機が停止するためにアクセス権限を変更するなどの例が挙げられる。アプリケーションプログラムからの指示とは、ユーザ情報管理装置１８０を実現する計算機や、ユーザ情報管理装置１８０が接続されている計算機で動くアプリケーションプログラムからの指示であり、例えば、アプリケーションプログラムの終了に伴い、アクセス権限を変更する指示が挙げられる。アクセス開始後経過時間とは、最初にアクセス１８１がアクセス受付部１８２で受け付けられてからの経過時間であり、アクセス放置時間と異なり、次にアクセスが受け付けられても０から経過時間の計測が開始されることはない。時刻情報とは、特定の時刻に到達したことを表す情報である。

アクセス拒絶回数とは、アクセス権判断部によってアクセス権限が無いと判断された回数であり、例えば、アクセス権限が無いと３回判断されると、別のアクセス権限へ変更することが実現できる。アクセス権限変更後経過時間とは、アクセス管理部１８５により、アクセスのデータに対するアクセス権限の変更が行われてからの経過時間である。アクセス権限の変更が行われて一定時間経過することにより、例えば、アクセス権限を低いもの、あるいは、アクセス権限がない状態にすることにより、ユーザ情報管理装置１８０に対してアクセスを受け付けさせたユーザが席をはずした後に、アクセス権限を低いもの、あるいは、アクセス権限がない状態になるので、他人がデータにアクセスしてしまうことを防止することができるようになる。

また、以上列挙した条件である、アクセス放置時間、データアクセス回数、アクセス者からの指示、オペレーティングシステムからの指示、アプリケーションプログラムからの指示、アクセス開始後経過時間、時刻情報、アクセス拒絶回数、アクセス権限変更後経過時間を二以上組み合わせることにより、データが他人によってアクセスされてしまうことをさらに予防することができる。例えば、アクセス放置時間を１時間３０分、アクセス開始後経過時間を２時間３０分、アクセス権限変更後経過時間を３時間と設定し、これらの時間を経過する条件が成立するとアクセス権限がない状態になるものとすると、午前８時に最初のアクセスが行われアクセス権限が高く変更され、２回目のアクセスが午前９時に３回目のアクセスが午前１０時に行われ、その後ユーザが席をはずして時刻が午前１１時になった場合、アクセス放置時間とアクセス開始後経過時間の条件は成立しないが、アクセス権限変更後経過時間の条件が成立するので、アクセス権限がない状態になり、他人がアクセスできないことになり、条件を二以上組み合わせることにより、安全性が高まる。

産業上の利用可能性

以上説明したように、本発明によれば、機器を構成する部品を識別する部品識別情報を有する部品情報を含む機器情報と、機器の映像を構成する映像データとを受け付ける機器情報受付部と、部品識別情報を有する部品提供情報を管理する情報管理部と、機器情報受付部で受け付けた機器情報が有する部品識別情報を含む部品提供情報を情報管理部から取得する情報取得部と、情報取得部で取得した部品提供情報の全部または一部の情報および映像データから、表示データを生成するデータ生成部とを備えたので、完成された製造品を構成する部品の情報を、製造品に関連付けて表示することにより、顧客の必要な情報を効率的かつ合理的に入手することが可能となる。

また、状態情報により、引き合いプロセス中の状態をも知ることができ、製品の企画開発に有効な情報を簡単に手に入れられる。さらには、アクセス者に応じて最適な情報開示範囲とするので、情報の拡散により自社に不利な状態を招来することを防止できる。

また、データに対するアクセスが受け付けられ、アクセス権限がないことによるエラーが発生しても、受け付けられたアクセスのデータに対するアクセス権限が変更されて操作をそのまま続行することができ、ユーザに再度アクセス権限を変更して同じ操作を再び繰り返させなくてもよいことになる。

請求の範囲

1．ユーザ端末と双方向通信が可能なサーバ上に、あるいは前記ユーザ端末に構築されたユーザ情報管理装置であって、前記ユーザ端末を利用する複数のユーザに関するユーザ情報をセキュリティレベルと関連づけて保持するための記憶手段と、前記ユーザが前記サーバにアクセスして、所定のアプリケーションを利用しようとしたとき、前記ユーザを識別する識別手段と、前記ユーザが前記サーバにアクセスしたとき、あらかじめ定められた複数の認証レベルのいずれの認証レベルであるかを判定するレベル判定手段と、前記記憶手段に保持されている前記ユーザ情報の中で、前記判定されたレベルに対応する前記セキュリティレベル及びそれ以下のセキュリティレベルのユーザ情報のみを前記ユーザ端末及び／又は他の装置に対して送信可能とする送信制御手段と、前記送信制御手段により送信可能とされた後、所定時間の経過及び／又は所定動作の実行後に、あるいは前記ユーザからの所定の指示に応じて前記送信可能とされたユーザ情報を送信不可能な状態とする送信禁止手段とを、有するユーザ情報管理装置。

2．前記送信禁止手段が、前記判定されたレベルに対応する前記セキュリティレベルより低いセキュリティレベルのユーザ情報のみを前記ユーザ端末及び／又は他の装置に対して送信可能とするものである請求の範囲第1項に記載のユーザ情報管理装置。

3．前記ユーザ識別手段が、前記ユーザ端末において前記ユーザが入力するパスワード、あるいは前記ユーザ端末が読み取るＩＣカード情報、磁気カード情報、前記ユーザの指紋、声紋、虹彩紋のうちいずれか1つ以上を用いるものである請求の範囲第1項又は請求の範囲第2項に記載のユーザ情報管理装置。

4．前記レベル判定手段が、前記ユーザがユーザ識別のために用いたあらかじめ定められた手法を判断することによりレベルを判定するものである請求の範囲第１項ないし請求の範囲第３項のいずれか１つに記載のユーザ情報管理装置。

5．前記ユーザ識別手段が、前記ユーザ端末において前記ユーザが操作する入力装置からの所定指示に基づき前記ユーザを判断し、この場合前記レベル判定手段が最も低い認証レベルであると判定する請求の範囲第１項ないし請求の範囲第４項のいずれか１つに記載のユーザ情報管理装置。

6．前記送信制御手段が、前記ユーザの現在の認証レベルが求められたデータ取得に必要な認証レベルより低い場合は、前記必要な認証レベルに引き上げるため前記ユーザに対して必要な行動をとるよう指示するものである請求の範囲第１項ないし請求の範囲第５項のいずれか１つに記載のユーザ情報管理装置。

7．前記送信制御手段が、前記ユーザ情報に固有のセキュリティレベルを定義する手段と、前記セキュリティレベル毎に前記ユーザ情報を管理する手段とを有するものである請求の範囲第１項ないし請求の範囲第６項のいずれか１つに記載のユーザ情報管理装置。

8．前記ユーザ端末を利用する複数のユーザに共通の情報をもグループデータとしてセキュリティレベルと関連づけて前記記憶手段に保持するよう構成された請求の範囲第１項ないし請求の範囲第７項のいずれか１つに記載のユーザ情報管理装置。

9．要求されたデータの集合に対して、その事象となる確率とデータ間の距離からＩＤとなる指数を求め、その値を用いてセキュリティを再チェックする手段を有する請求の範囲第１項ないし請求の範囲第８項のいずれか１つに記載のユーザ情報管理装置。

１０．前記複数のユーザ端末をあらかじめ複数のセキュリティ区分に分類しておき、セキュリティ区分判定手段を備えることにより、アクセスしてきた前記ユーザ端末のセキュリティ区分毎にアクセス制限を加えるよう構成した請求の範囲第１項ないし請求の範囲第９項のいずれか１つに記載のユーザ情報管理装置。

１１．前記ユーザ端末の前記セキュリティ区分を当該ユーザ端末の登録ユーザ数で決定するよう構成された請求の範囲第１０項に記載のユーザ情報管理装置。

１２．前記セキュリティ区分中、所定の区分に該当するときは、認証レベルが低いものに移行したときに、前記認証レベルが低いものに移行する以前に前記サーバから前記ユーザ端末に伝送したデータを削除するよう構成されている請求の範囲第１０項に記載のユーザ情報管理装置。

１３．前記セキュリティ区分中、所定の区分に該当するときは、前記ユーザ端末から前記サーバの所定作業エリアに対して前記ユーザ端末から入力されたデータを自動的及び／又は定期的に伝送するよう構成された請求の範囲第１０項に記載のユーザ情報管理装置。

１４．データを要求する側のユーザ情報利用基準をあらかじめ格納するユーザ情報利用基準格納手段と、データを提供する側のユーザ情報提供条件をあらかじめ格納するユーザ情報提供条件格納手段とを更に有し、前記送信制御手段がさらに、前記ユーザ情報利用基準と前記ユーザ情報提供条件とを比較し、比較結果により送信制御をする際に、データ中に前記ユーザ判定手段にて判断されたユーザ以外のユーザ情報が含まれている場合には、当該ユーザの前記ユーザ情報提供条件を求め、前記ユーザ情報利用基準との比較を行うことによって送信するか否かの判断をする請求の範囲第１項ないし請求の範囲第１３項のいずれか１つに記載のユーザ情報管理装置。

１５．ユーザ端末と双方向通信が可能なサーバ上に、あるいは前記ユーザ端末に構築されたユーザ情報管理装置におけるユーザ情報管理方法であって、前記ユーザ端末を利用する複数のユーザに関するユーザ情報をセキュリティレベルと関連づけて保持するための記憶ステップと、前記ユーザが前記サーバにアクセスして、所定のアプリケーションを利用しようとしたとき、前記ユーザを識別する識別ステップと、前記ユーザが前記サーバにアクセスしたとき、あらかじめ定められた複数の認証レベルのいずれの認証レベルであるかを判定するレベル判定ステップと、前記記憶ステップで保持された前記ユーザ情報の中で、前記判定されたレベルに対応する前記セキュリティレベル及びそれ以下のセキュリティレベルのユーザ情報のみを前記ユーザ端末及び／又は他の装置に対して送信可能とする送信制御ステップと、前記送信制御ステップにより送信可能とされた後、所定時間の経過及び／又は所定動作の実行後に、あるいは前記ユーザからの所定の指示に応じて前記送信可能とされたユーザ情報を送信不可能な状態とする送信禁止ステップとを、有するユーザ情報管理方法。

１６．前記送信禁止ステップが、前記判定されたレベルに対応する前記セキュリティレベルより低いセキュリティレベルのユーザ情報のみを前記ユーザ端末及び／又は他の装置に対して送信可能とするものである請求の範囲第１５項に記載のユーザ情報管理方法。

１７．前記ユーザ識別ステップが、前記ユーザ端末において前記ユーザが入力するパスワード、あるいは前記ユーザ端末が読み取るＩＣカード情報、磁気カード情報、前記ユーザの指紋、声紋、虹彩紋のうちいずれか１つ以上を用いるものである請求の範囲第１５項又は請求の範囲第１６項に記載のユーザ情報管理方法。

１８．前記レベル判定ステップが、前記ユーザがユーザ識別のために用

いたあらかじめ定められた手法を判断することによりレベルを判定するものである請求の範囲第１５項ないし請求の範囲第１７項のいずれか１つに記載のユーザ情報管理方法。

１９．前記ユーザ識別ステップが、前記ユーザ端末において前記ユーザが操作する入力装置からの所定指示に基づき前記ユーザを判断し、この場合前記レベル判定ステップが最も低い認証レベルであると判定する請求の範囲第１５項ないし請求の範囲第１８項のいずれか１つに記載のユーザ情報管理方法。

２０．前記送信制御ステップが、前記ユーザの現在の認証レベルが求められたデータ取得に必要な認証レベルより低い場合は、前記必要な認証レベルに引き上げるため前記ユーザに対して必要な行動をとるよう指示するものである請求の範囲第１５項ないし請求の範囲第１９項のいずれか１つに記載のユーザ情報管理方法。

２１．前記送信制御ステップが、前記ユーザ情報に固有のセキュリティレベルを定義するステップと、前記セキュリティレベル毎に前記ユーザ情報を管理するステップとを有するものである請求の範囲第１５項ないし請求の範囲第２０項のいずれか１つに記載のユーザ情報管理方法。

２２．前記ユーザ端末を利用する複数のユーザに共通の情報をもグループデータとしてセキュリティレベルと関連づけて前記記憶ステップで保持するよう構成された請求の範囲第１５項ないし請求の範囲第２１項のいずれか１つに記載のユーザ情報管理方法。

２３．要求されたデータの集合に対して、その事象となる確率とデータ間の距離からＩＤとなる指数を求め、その値を用いてセキュリティを再チェックするステップを有する請求の範囲第１５項ないし請求の範囲第２２項のいずれか１つに記載のユーザ情報管理方法。

２４．前記複数のユーザ端末をあらかじめ複数のセキュリティ区分に分

類しておき、セキュリティ区分判定ステップを備えることにより、アクセスしてきた前記ユーザ端末のセキュリティ区分毎にアクセス制限を加えるよう構成した請求の範囲第１５項ないし請求の範囲第２３項のいずれか１つに記載のユーザ情報管理方法。

２５．前記ユーザ端末の前記セキュリティ区分を当該ユーザ端末の登録ユーザ数で決定するよう構成された請求の範囲第２４項に記載のユーザ情報管理方法。

２６．前記セキュリティ区分中、所定の区分に該当するときは、認証レベルが低いものに移行したときに、前記認証レベルが低いものに移行する以前に前記サーバから前記ユーザ端末に伝送したデータを削除するよう構成されている請求の範囲第２４項に記載のユーザ情報管理方法。

２７．前記セキュリティ区分中、所定の区分に該当するときは、前記ユーザ端末から前記サーバの所定作業エリアに対して前記ユーザ端末から入力されたデータを自動的及び／又は定期的に伝送するよう構成された請求の範囲第２４項に記載のユーザ情報管理方法。

２８．データを要求する側のユーザ情報利用基準をあらかじめ格納しておき、またデータを提供する側のユーザ情報提供条件をあらかじめ格納しておき、前記送信制御ステップがさらに、前記ユーザ情報利用基準と前記ユーザ情報提供条件とを比較し、比較結果により送信制御をする際に、データ中に前記ユーザ判定手段にて判断されたユーザ以外のユーザ情報が含まれている場合には、当該ユーザの前記ユーザ情報提供条件を求め、前記ユーザ情報利用基準との比較を行うことによって送信するか否かの判断をする請求の範囲第１５項ないし請求の範囲第２７項のいずれか１つに記載のユーザ情報管理方法。

２９．ユーザ端末と双方向通信が可能なサーバ上に、あるいは前記ユーザ端末に構築されたユーザ情報管理装置におけるユーザ情報管理方法を

実行するための制御プログラムがコンピュータが読み取り可能な状態で記録された記録媒体であって、前記ユーザ端末を利用する複数のユーザに関するユーザ情報をセキュリティレベルと関連づけて保持するための記憶ステップと、前記ユーザが前記サーバにアクセスして、所定のアプリケーションを利用しようとしたとき、前記ユーザを識別する識別ステップと、前記ユーザが前記サーバにアクセスしたとき、あらかじめ定められた複数の認証レベルのいずれの認証レベルであるかを判定するレベル判定ステップと、前記記憶ステップで保持された前記ユーザ情報の中で、前記判定されたレベルに対応する前記セキュリティレベル及びそれ以下のセキュリティレベルのユーザ情報のみを前記ユーザ端末及び／又は他の装置に対して送信可能とする送信制御ステップと、前記送信制御ステップにより送信可能とされた後、所定時間の経過及び／又は所定動作の実行後に、あるいは前記ユーザからの所定の指示に応じて前記送信可能とされたユーザ情報を送信不可能な状態とする送信禁止ステップとを、有するユーザ情報管理方法を実行するための制御プログラムがコンピュータが読み取り可能な状態で記録された記録媒体。

３０．前記送信禁止ステップが、前記判定されたレベルに対応する前記セキュリティレベルより低いセキュリティレベルのユーザ情報のみを前記ユーザ端末及び／又は他の装置に対して送信可能とするものである請求の範囲第２９項に記載のユーザ情報管理方法を実行するための制御プログラムがコンピュータが読み取り可能な状態で記録された記録媒体。

３１．前記ユーザ識別ステップが、前記ユーザ端末において前記ユーザが入力するパスワード、あるいは前記ユーザ端末が読み取るＩＣカード情報、磁気カード情報、前記ユーザの指紋、声紋、虹彩紋のうちいずれか１つ以上を用いるものである請求の範囲第２９項又は請求の範囲第３０項に記載のユーザ情報管理方法を実行するための制御プログラムがコ

ンピュータが読み取り可能な状態で記録された記録媒体。

３２．前記レベル判定ステップが、前記ユーザがユーザ識別のために用いたあらかじめ定められた手法を判断することによりレベルを判定するものである請求の範囲第２９項ないし請求の範囲第３１項のいずれか１つに記載のユーザ情報管理方法を実行するための制御プログラムがコンピュータが読み取り可能な状態で記録された記録媒体。

３３．前記ユーザ識別ステップが、前記ユーザ端末において前記ユーザが操作する入力装置からの所定指示に基づき前記ユーザを判断し、この場合前記レベル判定ステップが最も低い認証レベルであると判定する請求の範囲第２９項ないし請求の範囲第３２項のいずれか１つに記載のユーザ情報管理方法を実行するための制御プログラムがコンピュータが読み取り可能な状態で記録された記録媒体。

３４．前記送信制御ステップが、前記ユーザの現在の認証レベルが求められたデータ取得に必要な認証レベルより低い場合は、前記必要な認証レベルに引き上げるため前記ユーザに対して必要な行動をとるよう指示するものである請求の範囲第２９項ないし請求の範囲第３３項のいずれか１つに記載のユーザ情報管理方法を実行するための制御プログラムがコンピュータが読み取り可能な状態で記録された記録媒体。

３５．前記送信制御ステップが、前記ユーザ情報に固有のセキュリティレベルを定義するステップと、前記セキュリティレベル毎に前記ユーザ情報を管理するステップとを有するものである請求の範囲第２９項ないし請求の範囲第３４項のいずれか１つに記載のユーザ情報管理方法を実行するための制御プログラムがコンピュータが読み取り可能な状態で記録された記録媒体。

３６．前記ユーザ端末を利用する複数のユーザに共通の情報をもグループデータとしてセキュリティレベルと関連づけて前記記憶ステップにて

保持するよう構成された請求の範囲第２９項ないし請求の範囲第３５項のいずれか１つに記載のユーザ情報管理方法を実行するための制御プログラムがコンピュータが読み取り可能な状態で記録された記録媒体。

３７．要求されたデータの集合に対して、その事象となる確率とデータ間の距離からＩＤとなる指数を求め、その値を用いてセキュリティを再チェックするステップを有する請求の範囲第２９項ないし請求の範囲第３６項のいずれか１つに記載のユーザ情報管理方法を実行するための制御プログラムがコンピュータが読み取り可能な状態で記録された記録媒体。

３８．前記複数のユーザ端末をあらかじめ複数のセキュリティ区分に分類しておき、セキュリティ区分判定ステップを備えることにより、アクセスしてきた前記ユーザ端末のセキュリティ区分毎にアクセス制限を加えるよう構成した請求の範囲第２９項ないし請求の範囲第３７項のいずれか１つに記載のユーザ情報管理方法を実行するための制御プログラムがコンピュータが読み取り可能な状態で記録された記録媒体。

３９．前記ユーザ端末の前記セキュリティ区分を当該ユーザ端末の登録ユーザ数で決定するよう構成された請求の範囲第３８項に記載のユーザ情報管理方法を実行するための制御プログラムがコンピュータが読み取り可能な状態で記録された記録媒体。

４０．前記セキュリティ区分中、所定の区分に該当するときは、認証レベルが低いものに移行したときに、前記認証レベルが低いものに移行する以前に前記サーバから前記ユーザ端末に伝送したデータを削除するよう構成されている請求の範囲第３８項に記載のユーザ情報管理方法を実行するための制御プログラムがコンピュータが読み取り可能な状態で記録された記録媒体。

４１．前記セキュリティ区分中、所定の区分に該当するときは、前記ユ

ーザ端末から前記サーバの所定作業エリアに対して前記ユーザ端末から入力されたデータを自動的及び／又は定期的に伝送するよう構成された請求の範囲第３８項に記載のユーザ情報管理方法を実行するための制御プログラムがコンピュータが読み取り可能な状態で記録された記録媒体。

４２．データを要求する側のユーザ情報利用基準をあらかじめ格納しておき、またデータを提供する側のユーザ情報提供条件をあらかじめ格納しておき、前記ユーザ情報利用基準と前記ユーザ情報提供条件とを比較し、比較結果により送信制御をする際に、データ中に前記ユーザ判定手段にて判断されたユーザ以外のユーザ情報が含まれている場合には、当該ユーザの前記ユーザ情報提供条件を求め、前記ユーザ情報利用基準との比較を行うことによって送信するか否かの判断をする請求の範囲第２９項ないし請求の範囲第４１項のいずれか１つに記載のユーザ情報管理方法を実行するための制御プログラムがコンピュータが読み取り可能な状態で記録された記録媒体。

４３．データへのアクセスを受け付けるアクセス受付部と、アクセス受付部で受け付けたアクセスのデータに対するアクセス権限の有無を判断するアクセス権判断部と、アクセス受付部で受け付けたアクセスのデータに対するアクセス権限の変更を行うアクセス管理部とからなるユーザ情報管理装置。

４４．アクセス権判断部は、データと、アクセス権限とを関連付けたアクセス権限テーブルに基づいてアクセス権限の有無を判断する請求の範囲第４３項に記載のユーザ情報管理装置。

４５．アクセス権判断部は、データに記述されているアクセス権限に基づいてアクセス権限の有無を判断する請求の範囲第４３項に記載のユーザ情報管理装置。

４６．アクセス管理部は、変更されたアクセス権限を示す情報であるア

クセス権限変更情報を出力するアクセス権限変更情報出力手段を有する請求の範囲第４３項に記載のユーザ情報管理装置。

４７．アクセス権判断部は、アクセス権限変更情報出力手段からアクセス権限変更情報を取得するアクセス権限変更情報取得手段を有する請求の範囲第４６項に記載のユーザ情報管理装置。

４８．アクセス受付部は、機器からアクセスを受け付け、アクセス権限変更情報出力手段は、アクセス権限変更情報を、アクセス受付部にてアクセスを受け付けている機器に送信する請求の範囲第４６項に記載のユーザ情報管理装置。

４９．アクセス権限の変更のための条件を取得するアクセス権限変更条件取得部をさらに有する請求の範囲第４３項に記載のユーザ情報管理装置。

５０．アクセス管理部におけるアクセス権限の変更は、アクセスすることができるデータの範囲であるアクセスレベルの権限の変更である請求の範囲第４３項から請求の範囲第４７項に記載のユーザ情報管理装置。

５１．アクセスされるデータは、所有者毎に類別され、アクセス権限の変更は、アクセスしているデータに関連付けられている別の所有者のデータへするアクセスの変更である請求の範囲第４３項から請求の範囲第４７項のいずれか一に記載のユーザ情報管理装置。

５２．アクセス管理部は、前記アクセスの変更による処理の終了後に、元アクセス権限に復帰することを特徴とする請求の範囲第５１項に記載のユーザ情報管理装置。

５３．アクセス受付部でのアクセスが権限のないものであるとアクセス権判断部にて判断された場合に、アクセス権限の取得を要求する認証取得部をさらに有する請求の範囲第４３項から請求の範囲第４７項に記載のユーザ情報管理装置。

５４．前記アクセス権限の変更のための条件は、アクセス放置時間、データアクセス回数、アクセス者からの指示、オペレーティングシステムからの指示、アプリケーションプログラムからの指示、アクセス開始後経過時間、時刻情報、アクセス拒絶回数、アクセス権限変更後経過時間のいずれか一または二以上の組み合わせからなる条件である請求の範囲第４９項に記載のユーザ情報管理装置。

５５．データへのアクセスを受け付けるアクセス受付ステップと、アクセス受付ステップで受け付けられたアクセスのデータに対するアクセス権限の有無を判断するアクセス権判断ステップと、アクセス受付ステップで受け付けられたアクセスのデータに対するアクセス権限の変更を行うアクセス管理ステップとを計算機に実行させるユーザ情報管理プログラム。

５６．アクセス管理ステップにおいては、変更されたアクセス権限を示す情報であるアクセス権限変更情報を出力するアクセス権限変更情報出力ステップを計算機に実行させる請求の範囲第５５項に記載のユーザ情報管理プログラム。

５７．アクセス権限の変更のための条件を取得するアクセス権限変更条件取得ステップを計算機に実行させる請求の範囲第５５項に記載のユーザ情報管理プログラム。

図1

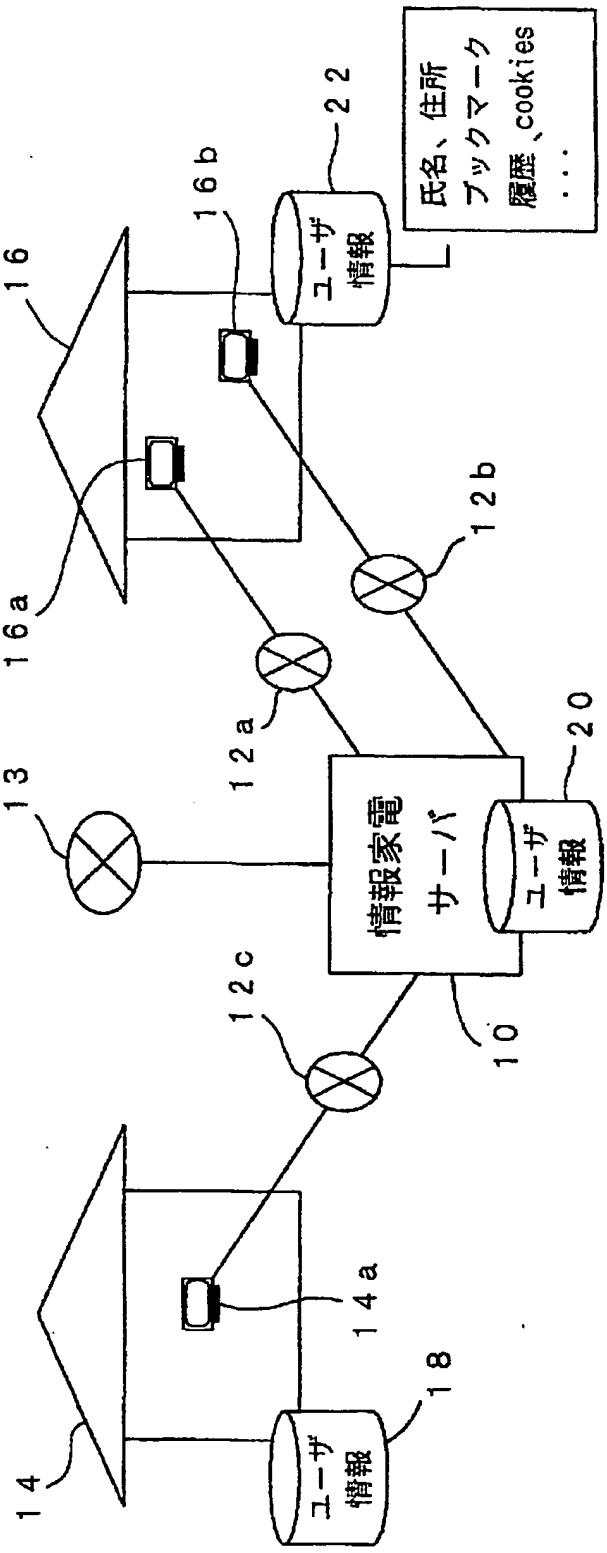

氏名、住所
ブックマーク
履歴、cookies
・・・
22
ユーザ情報
16b
16
16a
12b
12a
13
情報家電サーバ
20
ユーザ情報
12c
10
14a
18
ユーザ情報
14

図2

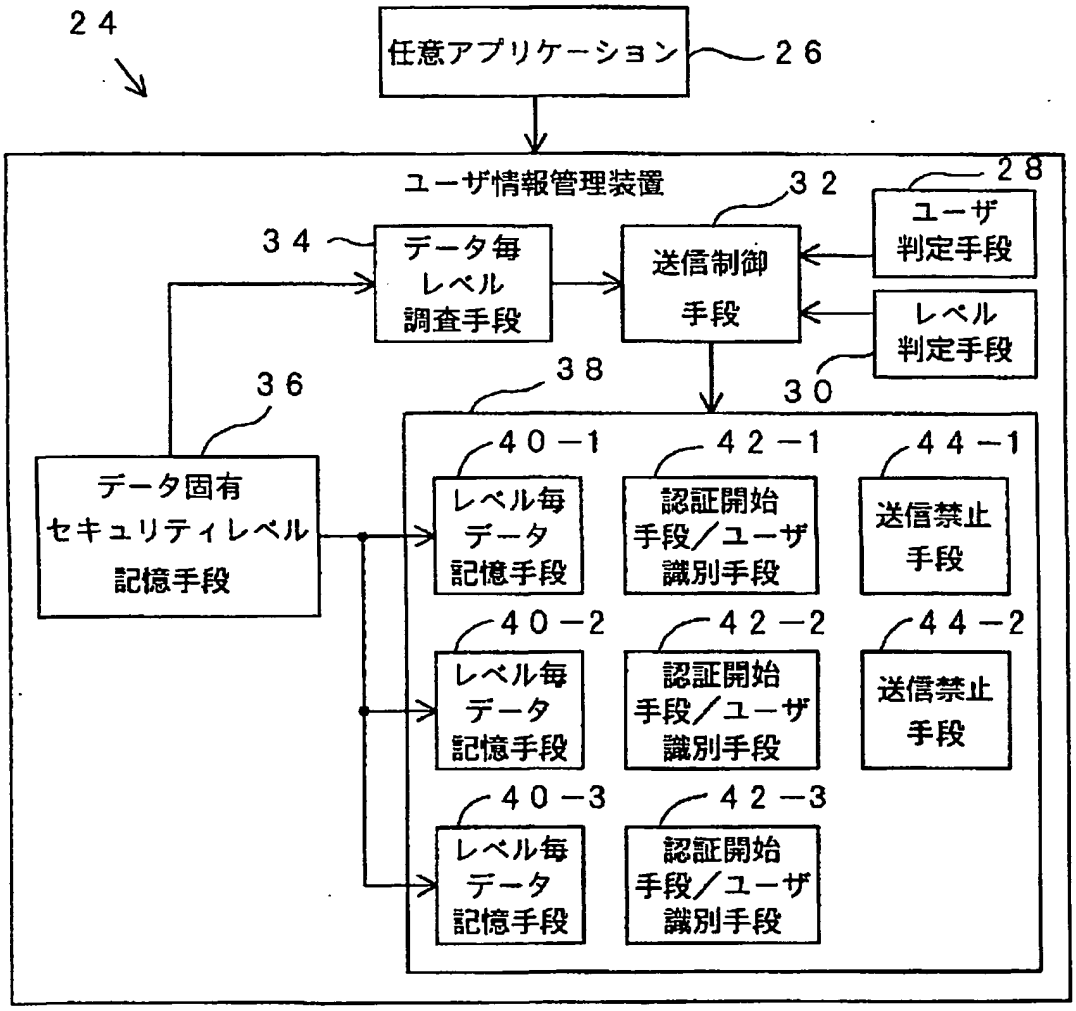

24
任意アプリケーション
26
ユーザ情報管理装置
28
32
ユーザ
判定手段
34
データ毎
レベル
調査手段
送信制御
手段
レベル
判定手段
30
38
36
データ固有
セキュリティレベル
記憶手段
40－1
42－1
44－1
レベル毎
データ
記憶手段
認証開始
手段／ユーザ
識別手段
送信禁止
手段
40－2
42－2
44－2
レベル毎
データ
記憶手段
認証開始
手段／ユーザ
識別手段
送信禁止
手段
40－3
42－3
レベル毎
データ
記憶手段
認証開始
手段／ユーザ
識別手段

図３

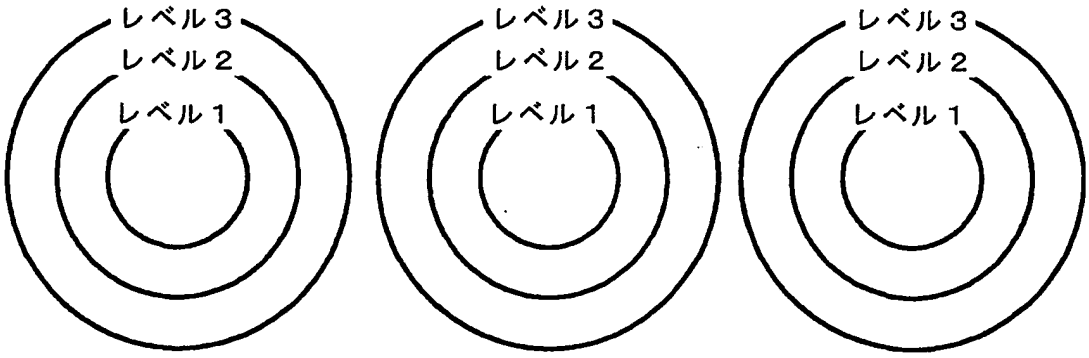


図４

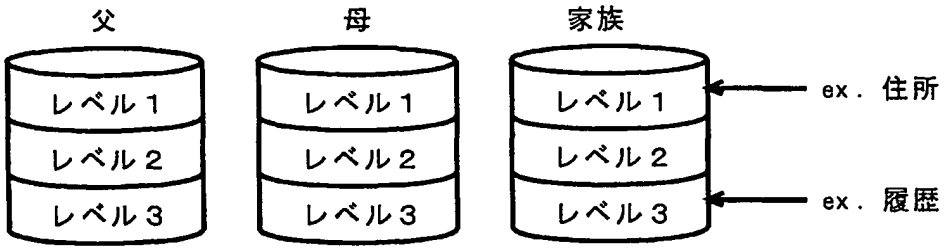


図５

例：母がレベル２でアクセスしたときのデータスコープ

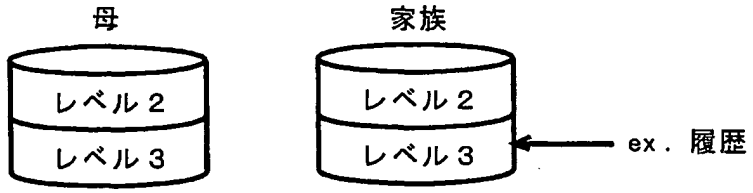


図6

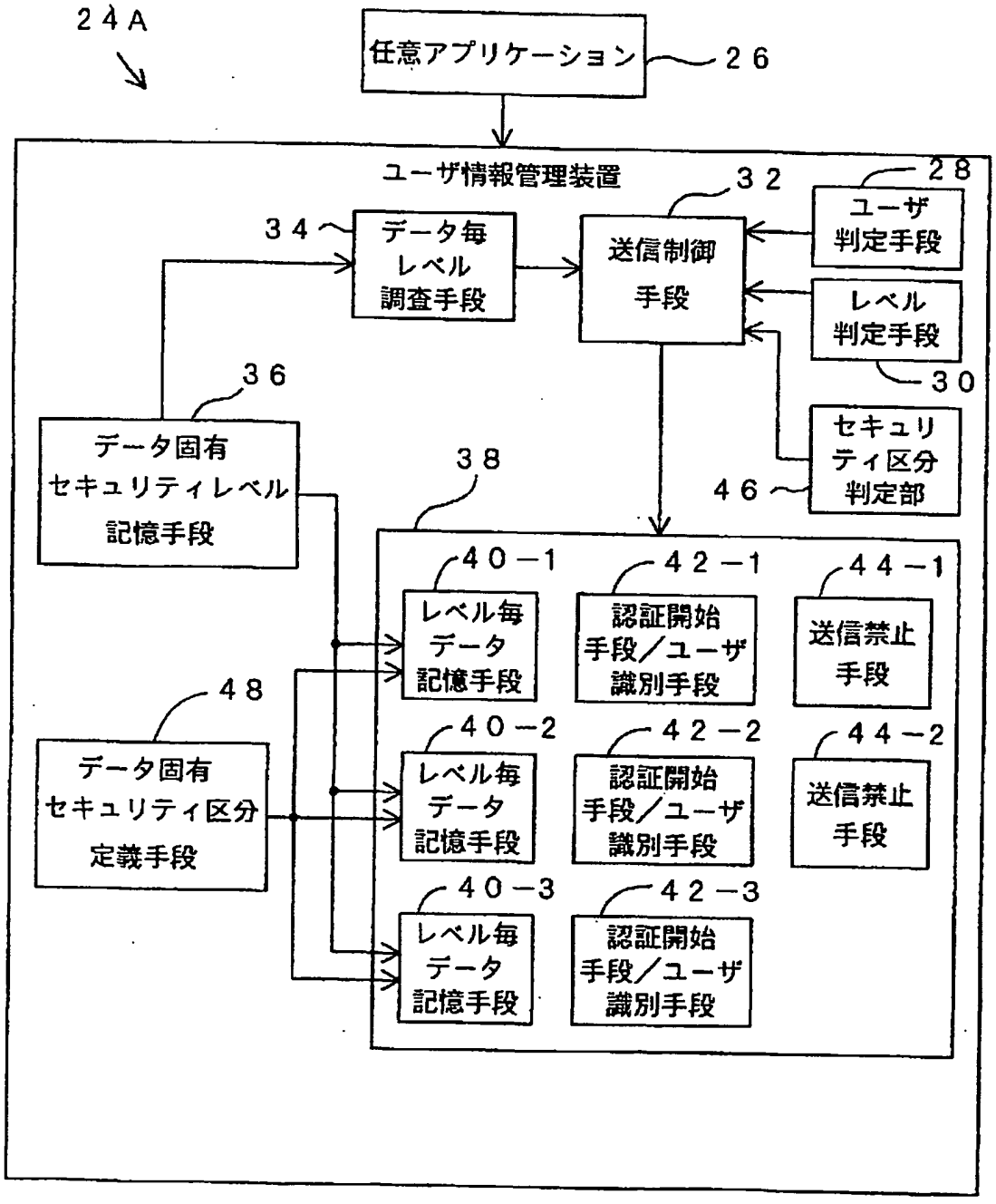

24A
任意アプリケーション
26
ユーザ情報管理装置
32
28
ユーザ判定手段
34
データ毎レベル調査手段
送信制御手段
レベル判定手段
30
36
データ固有セキュリティレベル記憶手段
セキュリティ区分判定部
46
38
40−1
42−1
44−1
レベル毎データ記憶手段
認証開始手段／ユーザ識別手段
送信禁止手段
48
40−2
42−2
44−2
データ固有セキュリティ区分定義手段
レベル毎データ記憶手段
認証開始手段／ユーザ識別手段
送信禁止手段
40−3
42−3
レベル毎データ記憶手段
認証開始手段／ユーザ識別手段

図7

データ属性定義

```
<User accessLevel="2" >
    <Name jp-description="氏名" >
        <First type="text" jp-description="姓" probability="0.00001" />
        <Last type="text" jp-description="名" probability="0.00001" />
    </Name>
    <Bdate jp-description="生年月日" probability="0.00274" >
        <Ymd>
            <Year type="number" jp-description="年" />
            <Month type=" number" jp-description="月" />
            <Day type=" number" jp-description="日" />
        </Ymd>
    </Bdate>
    <Gender type="gender" jp-description="性別" probability="0.5" />
</User>
<Dynamic accessLevel="3" >
    < ClickStream />
        <Client type="text" />
        <Server type="text" />
    </ClickStream>
</Dynamic>
```

図8

個人別データ

```
<User>
    <Name >
        <First value="田中" />
        <Last value="和子" />
    </Name>
    <Gender accessLevel="1" value="女" />
</User>
<Dynamic>
    < ClickStream />
        <Client type="http://www.foo.com/bar1.html" />
        <Client type="http://www.foo.com/bar2.html" />
    </ClickStream>
</Dynamic>
```

図9

レベル1のインスタンスが生成したデータ

```
<User>
    <Gender accessLevel="1" value="女" />
</User>
```

図 10

レベル2のインスタンスが生成したデータ

```
<User accessLevel="2">
    <Name >
        <First value="田中" />
        <Last value="和子" />
    </Name>
</User>
```

図 11

レベル3のインスタンスが生成したデータ

```
<Dynamic accessLevel="3" >
    < ClickStream />
        <Client type="htttp://www.foo.com/bar1.html" />
        <Client type="htttp://www.foo.com/bar2.html" />
    </ClickStream>
</Dynamic>
```

図12

レベル1

ユーザＩＤ	データ名	値
0000001	User.Gender	女

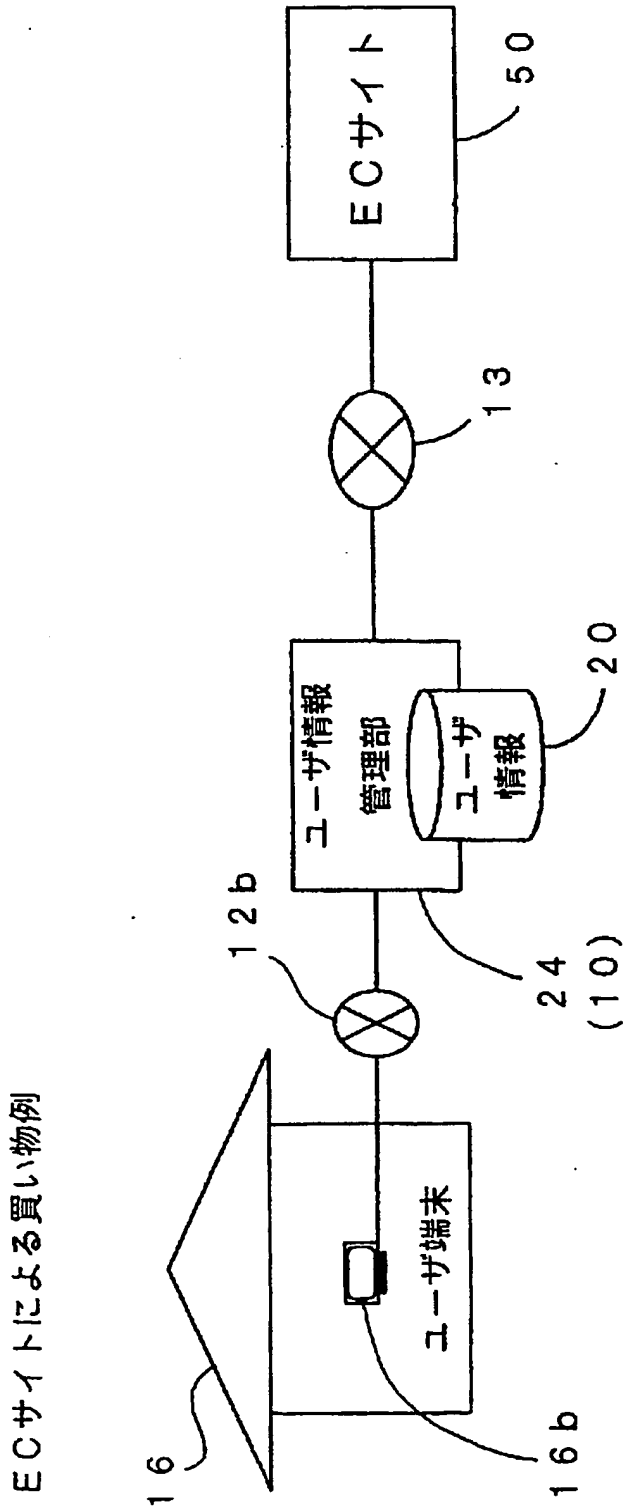
レベル2

ユーザＩＤ	データ名	値
0000001	User.Name.First	田中
0000001	User.Name.Last	花子
0000002	User.Name.First	渡辺
0000002	User.Name.Last	太郎
0000002	User.Gender	男

レベル3

ユーザＩＤ	データ名	値
0000001	Dynamic.ClickStream.Client	http://www.foo.com/bar1.html
0000001	Dynamic.ClickStream.Client	http://www.foo.com/bar2.html
0000002	Dynamic.ClickStream.Client	http://www.aaa.co.jp/bbb/ccc.html

図13



ECサイトによる買い物例

図１４

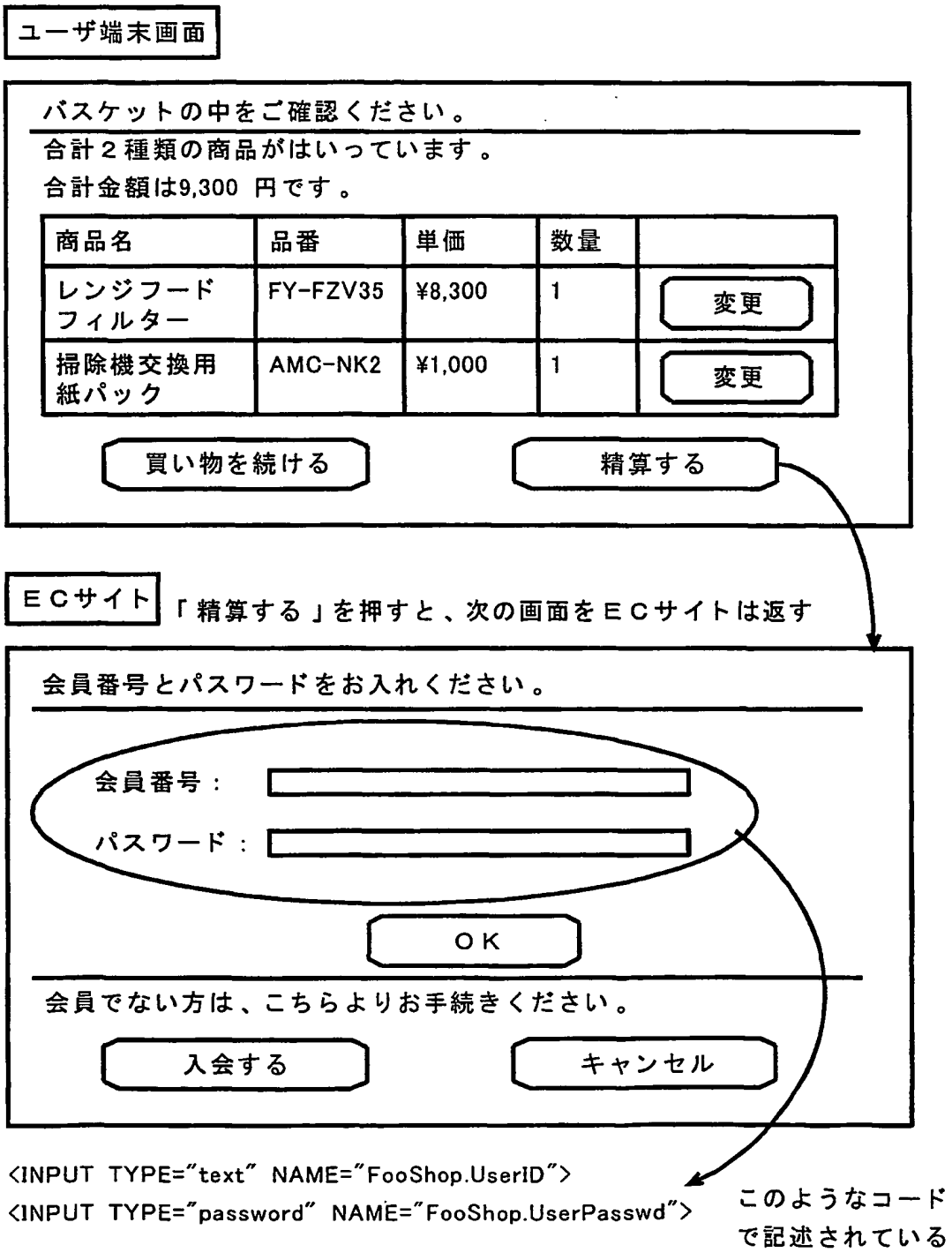

ユーザ端末画面
バスケットの中をご確認ください。
合計２種類の商品がはいっています。
合計金額は9,300 円です。
商品名
品番
単価
数量
レンジフード フィルター
FY-FZV35
¥8,300
1
変更
掃除機交換用 紙パック
AMC-NK2
¥1,000
1
変更
買い物を続ける
精算する
ＥＣサイト
「精算する」を押すと、次の画面をＥＣサイトは返す
会員番号とパスワードをお入れください。
会員番号：
パスワード：
ＯＫ
会員でない方は、こちらよりお手続きください。
入会する
キャンセル
<INPUT TYPE="text" NAME="FooShop.UserID">
<INPUT TYPE="password" NAME="FooShop.UserPasswd">
このようなコードで記述されている

図15

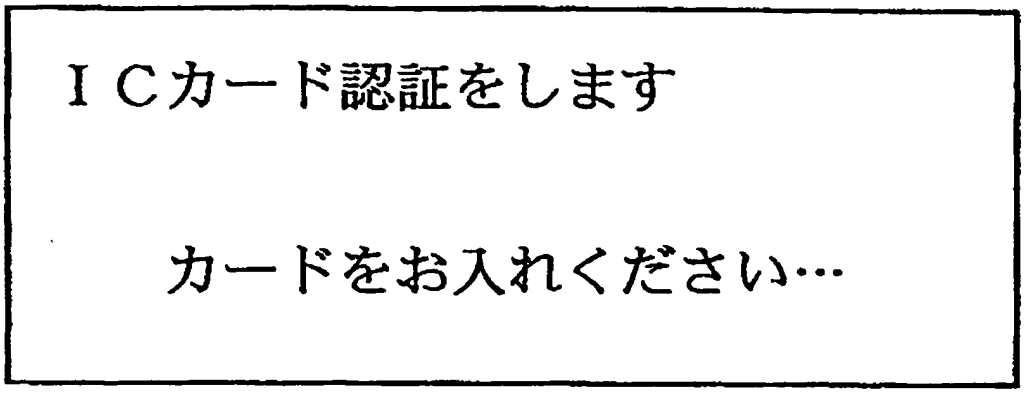
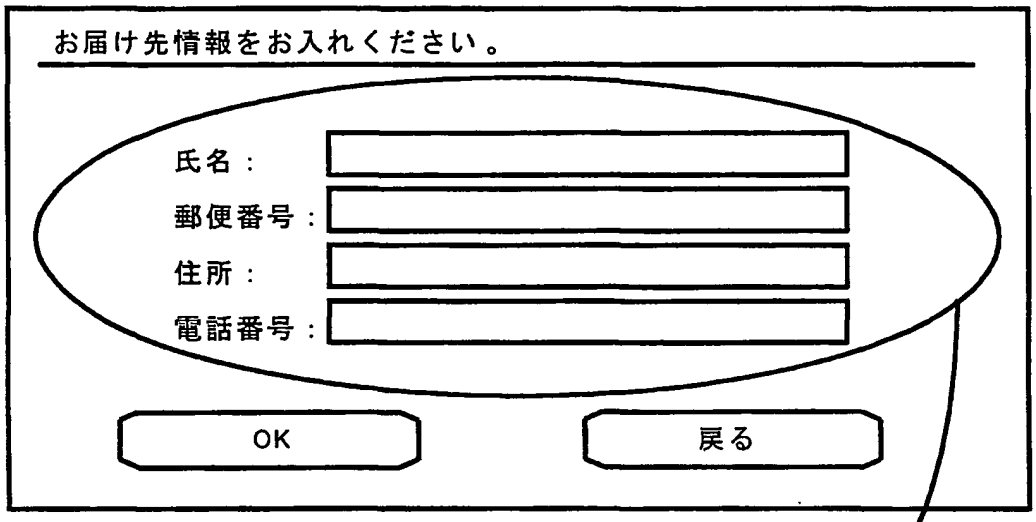


図１６




```
<INPUT TYPE="text" NAME="User.Name">
<INPUT TYPE="text" NAME="User.Postal.Postalcode">
<INPUT TYPE="text" NAME="User.Postal.Formatted">
<INPUT TYPE="text" NAME="User.Telecom.Telephone">
```

このようなコードで記述されている

図１７

```
<INPUT TYPE="text" NAME="User.Name" value="山田太郎">
<INPUT TYPE="text" NAME="User.Postal.Postalcode" value="123-0000">
<INPUT TYPE="text" NAME="User.Postal.Formatted" value="東京都･･･">
<INPUT TYPE="text" NAME="User.Telecom.Telephone" value="03-1234-5678">
```

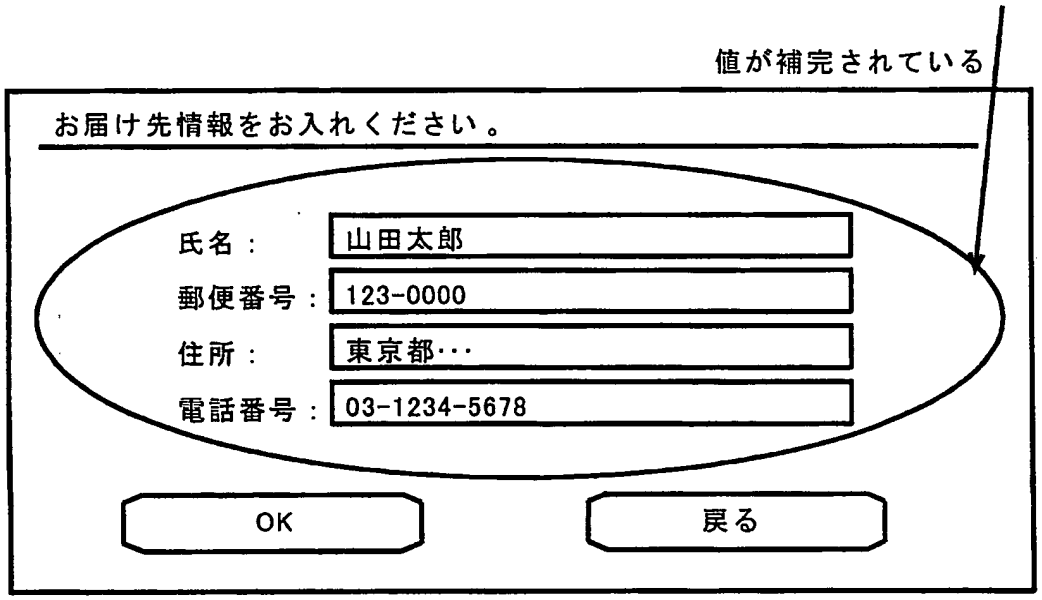


図１８

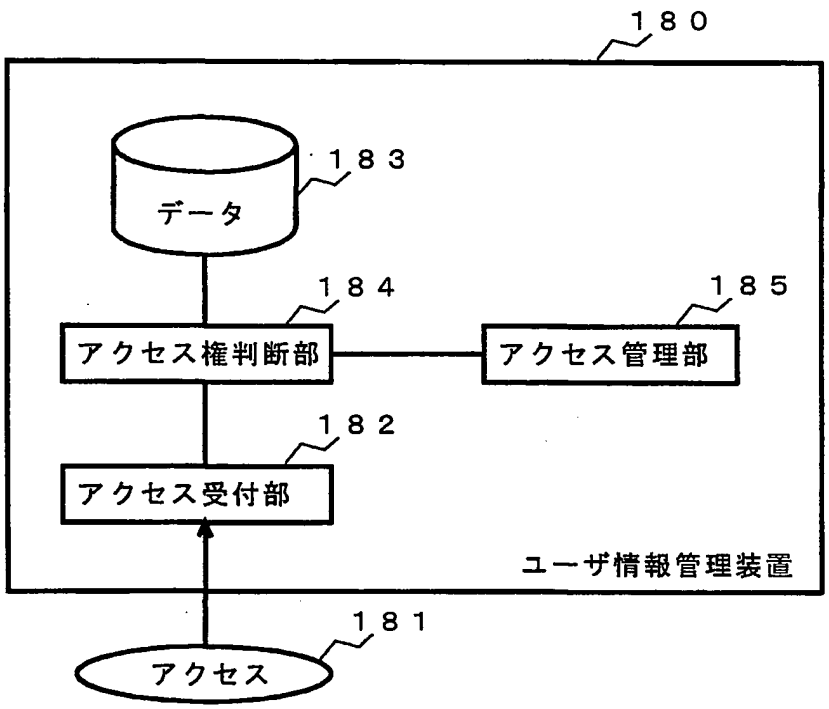

１８０
１８３
データ
１８４
１８５
アクセス権判断部
アクセス管理部
１８２
アクセス受付部
ユーザ情報管理装置
１８１
アクセス

図１９

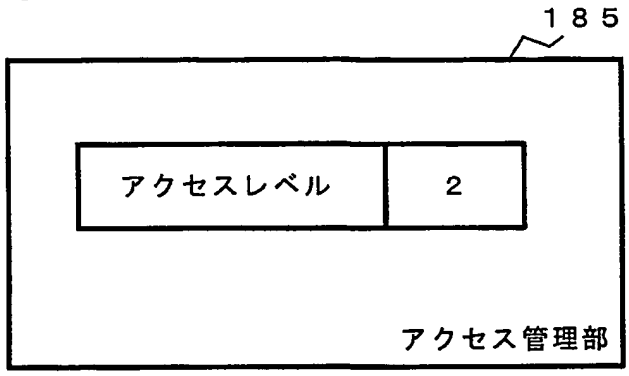


図２０

データ名	必要アクセスレベル
データＡ	1
データＢ	2
データＣ	3
⋮	⋮

図２１

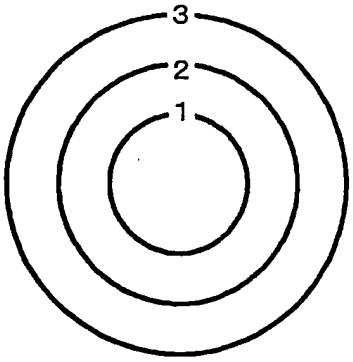


図２２

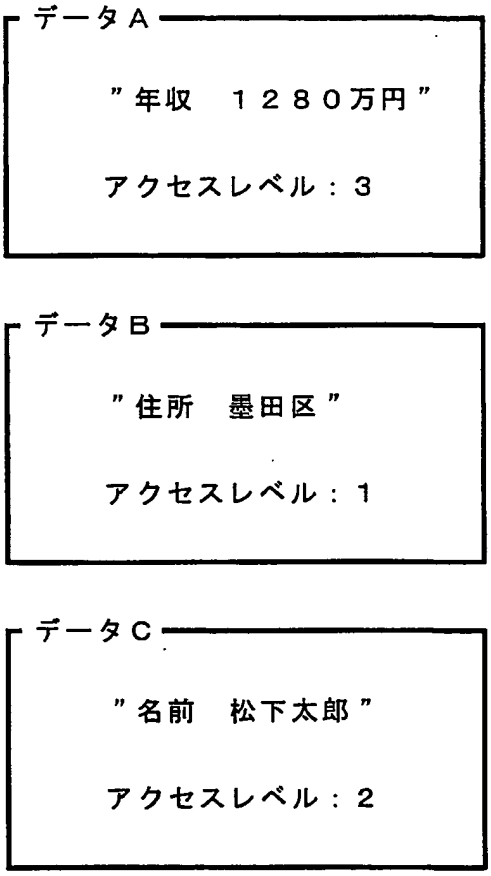

データＡ
”年収　１２８０万円”
アクセスレベル：３
データＢ
”住所　墨田区”
アクセスレベル：１
データＣ
”名前　松下太郎”
アクセスレベル：２

図２３

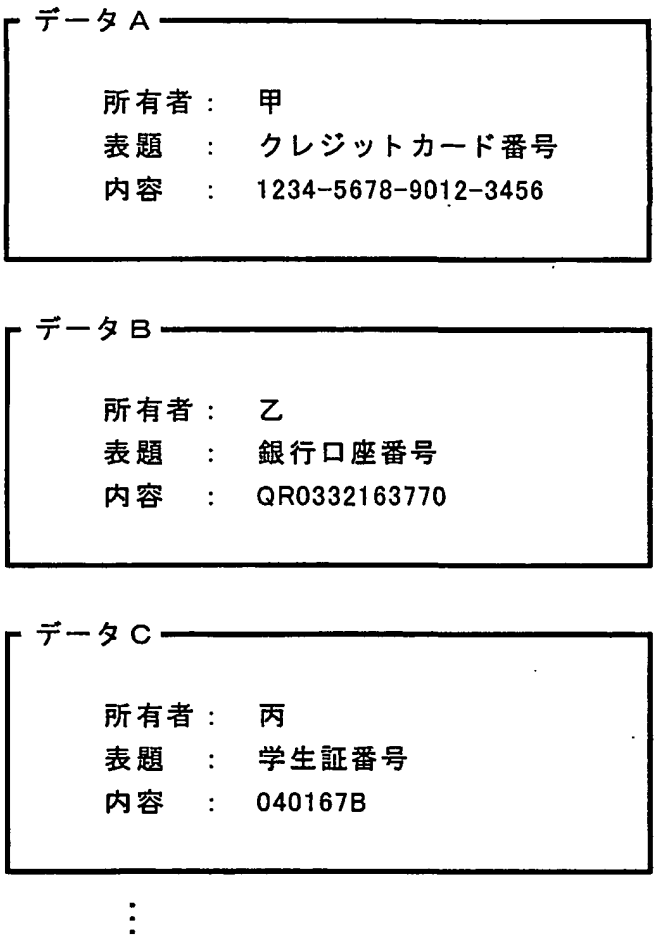

データＡ
所有者： 甲
表題 ： クレジットカード番号
内容 ： 1234-5678-9012-3456
データＢ
所有者： 乙
表題 ： 銀行口座番号
内容 ： QR0332163770
データＣ
所有者： 丙
表題 ： 学生証番号
内容 ： 040167B
⋮

図２４

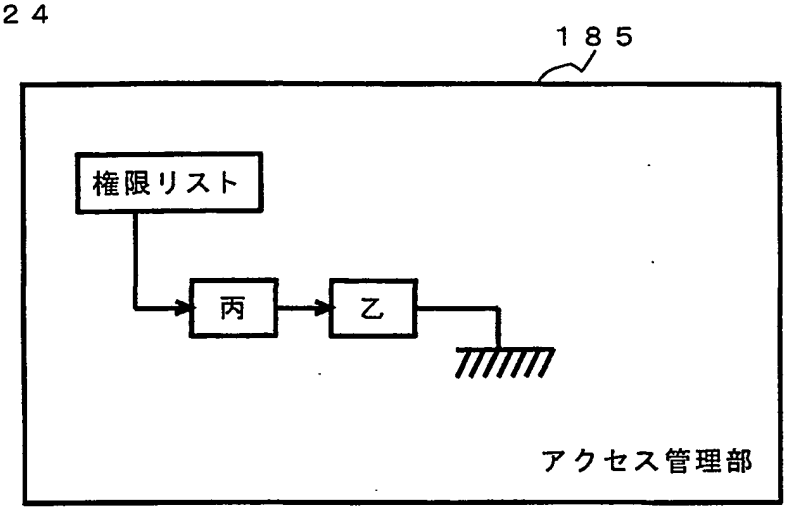


図２５

アクセス権限	データ表題	データ所有者
丙	クレジットカード番号	甲
丙	銀行口座番号	乙
⋮	⋮	⋮

図２６

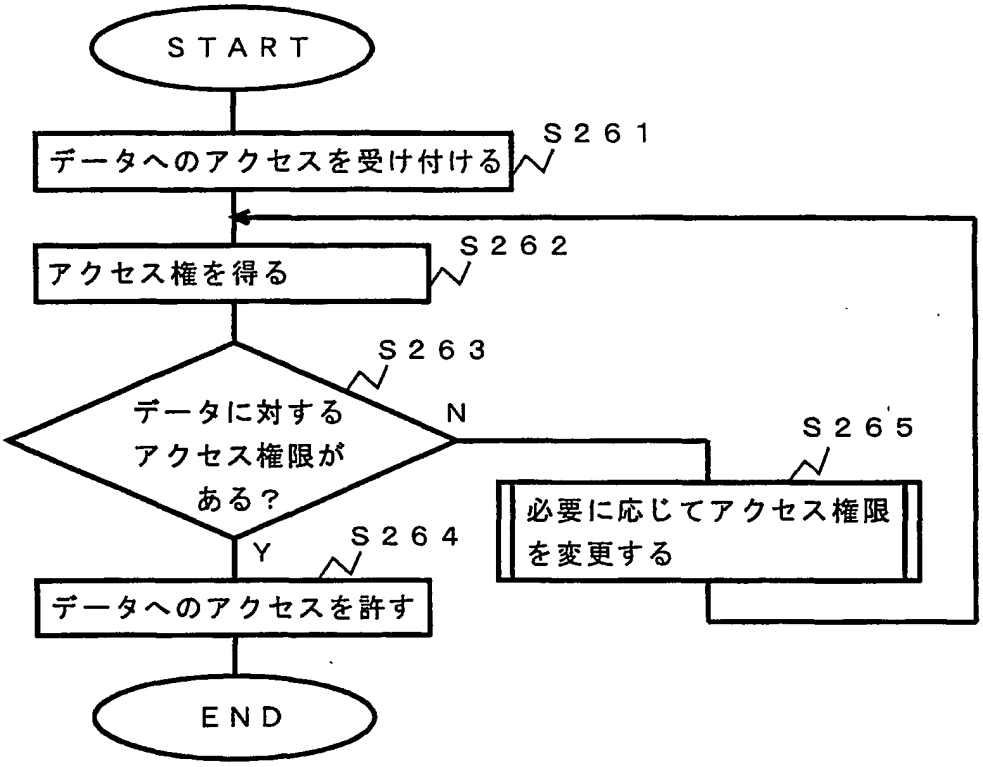

START
データへのアクセスを受け付ける
S２６１
アクセス権を得る
S２６２
S２６３
データに対する
アクセス権限が
ある？
N
S２６５
必要に応じてアクセス権限
を変更する
Y
S２６４
データへのアクセスを許す
END

図２７

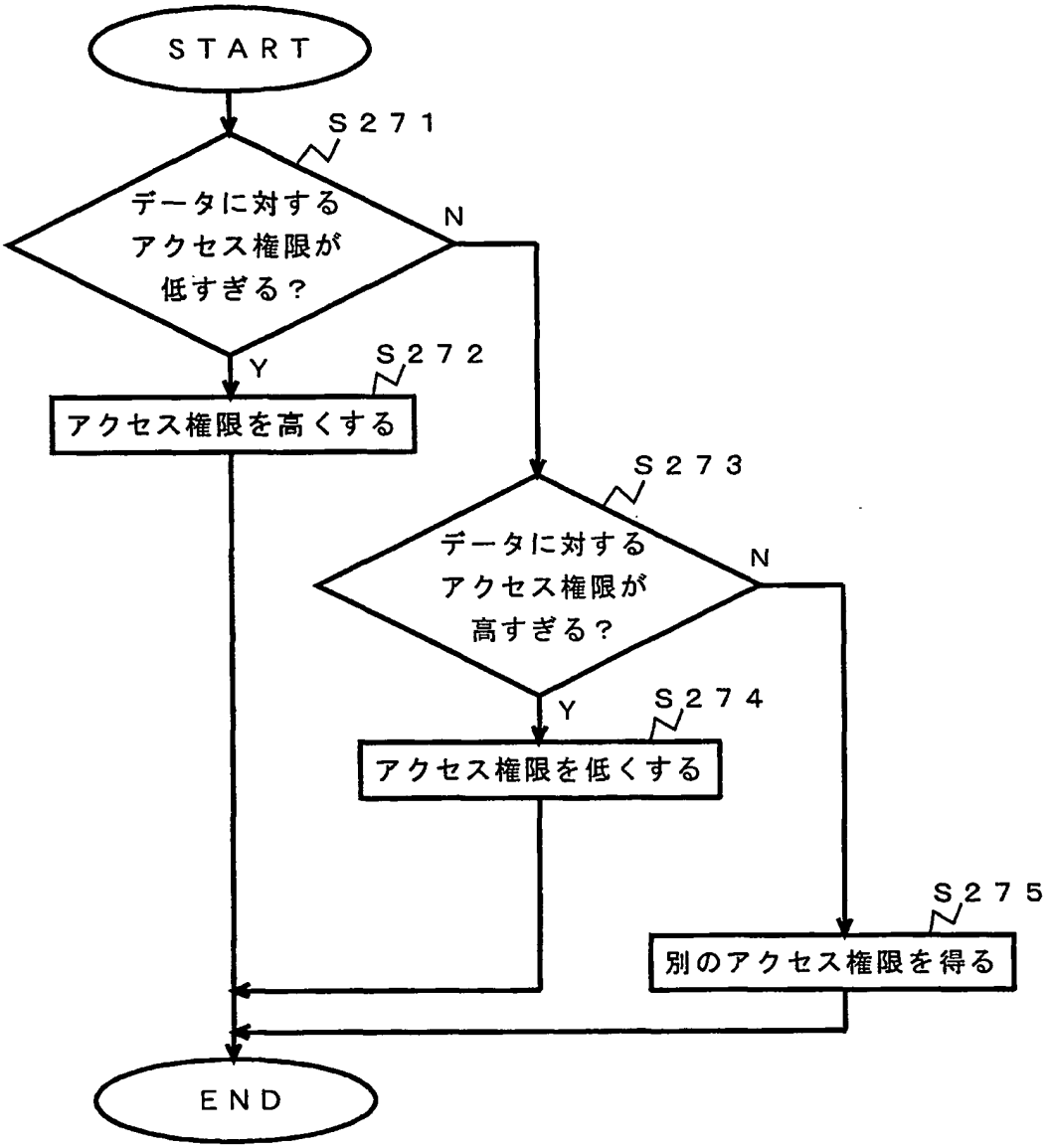

START
S２７１
データに対する
アクセス権限が
低すぎる？
N
Y
S２７２
アクセス権限を高くする
S２７３
データに対する
アクセス権限が
高すぎる？
N
Y
S２７４
アクセス権限を低くする
S２７５
別のアクセス権限を得る
END

図２８

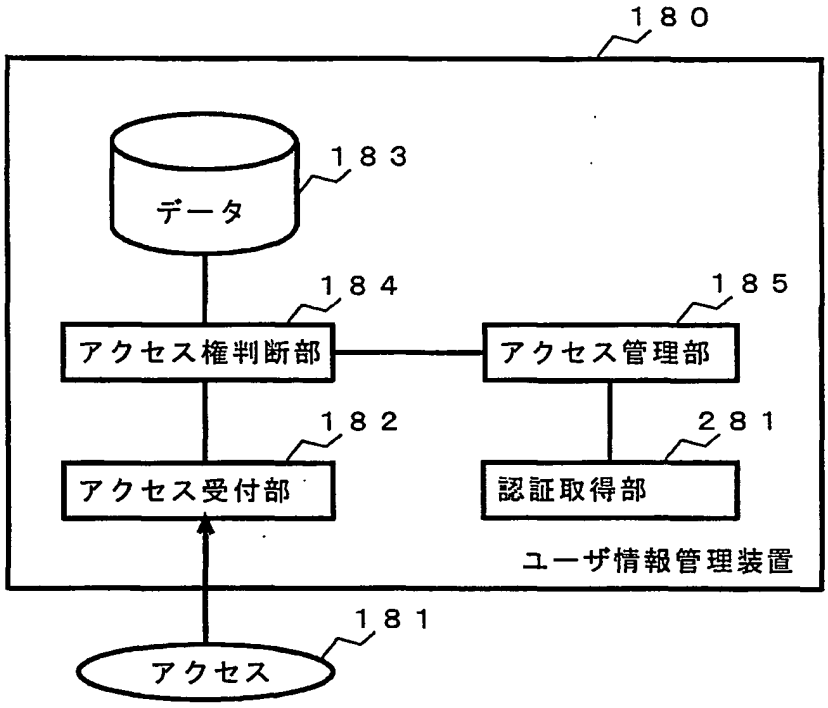

１８０
１８３
データ
１８４
アクセス権判断部
１８５
アクセス管理部
１８２
アクセス受付部
２８１
認証取得部
ユーザ情報管理装置
１８１
アクセス

図２９

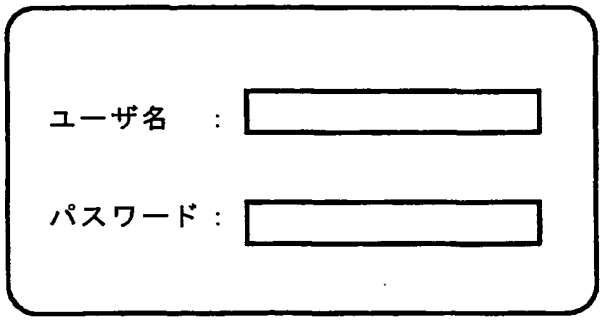


図３０

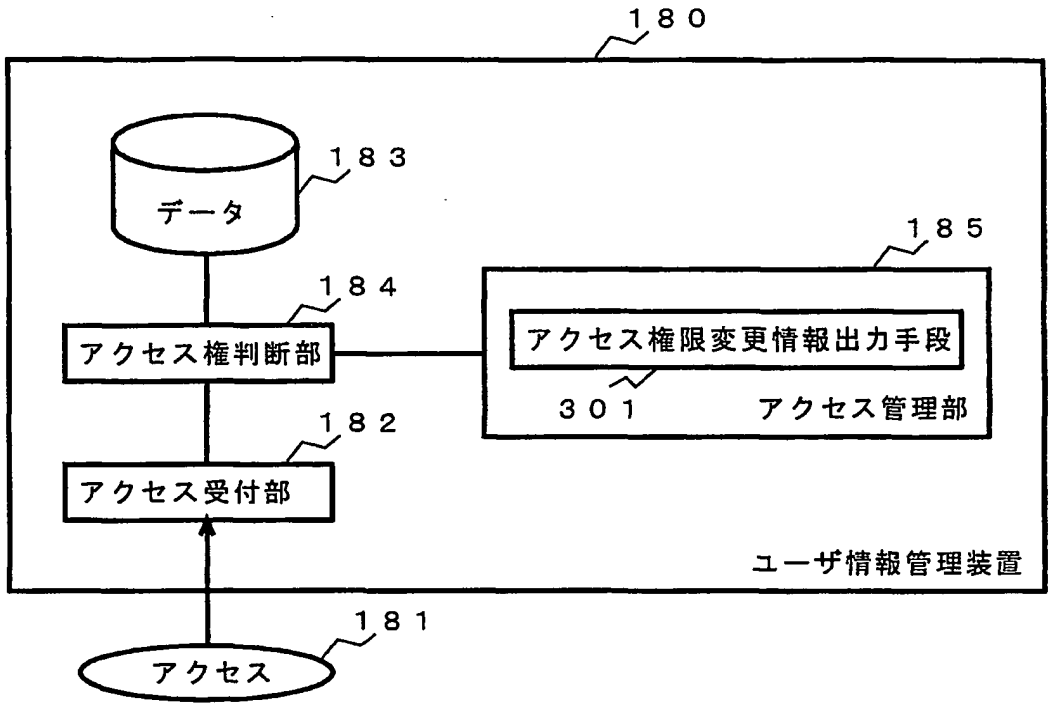

１８０
１８３
データ
１８５
１８４
アクセス権判断部
アクセス権限変更情報出力手段
３０１
アクセス管理部
１８２
アクセス受付部
ユーザ情報管理装置
１８１
アクセス

図３１

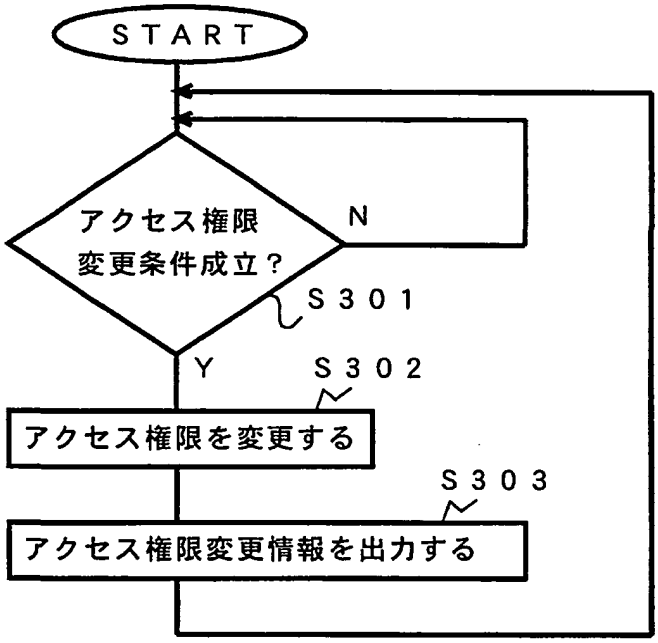

START
アクセス権限
変更条件成立？
N
Ｓ３０１
Y
Ｓ３０２
アクセス権限を変更する
Ｓ３０３
アクセス権限変更情報を出力する

図３２

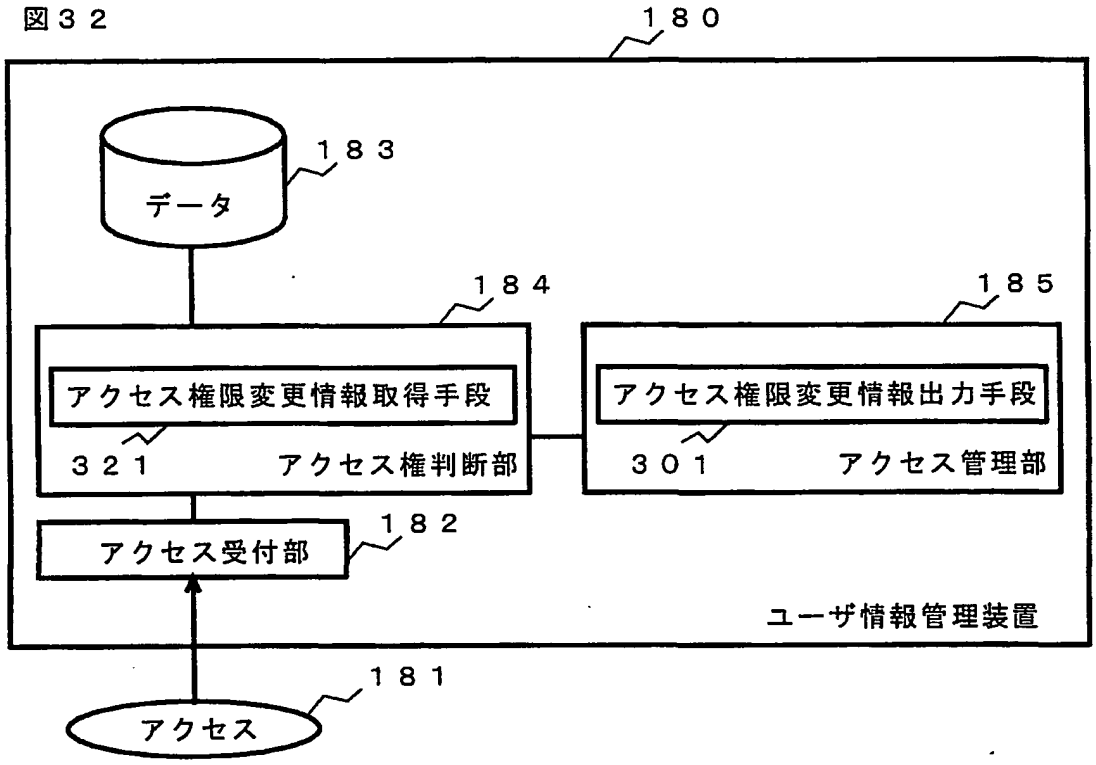

１８０
１８３
データ
１８４
１８５
アクセス権限変更情報取得手段
３２１
アクセス権判断部
アクセス権限変更情報出力手段
３０１
アクセス管理部
１８２
アクセス受付部
ユーザ情報管理装置
１８１
アクセス

図３３

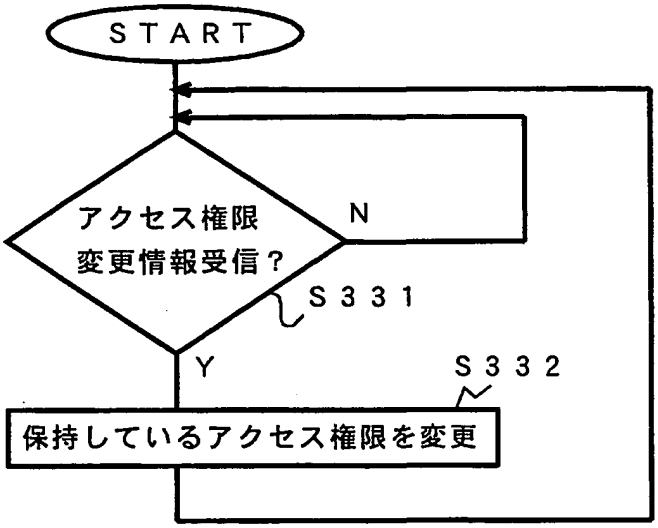


図３４

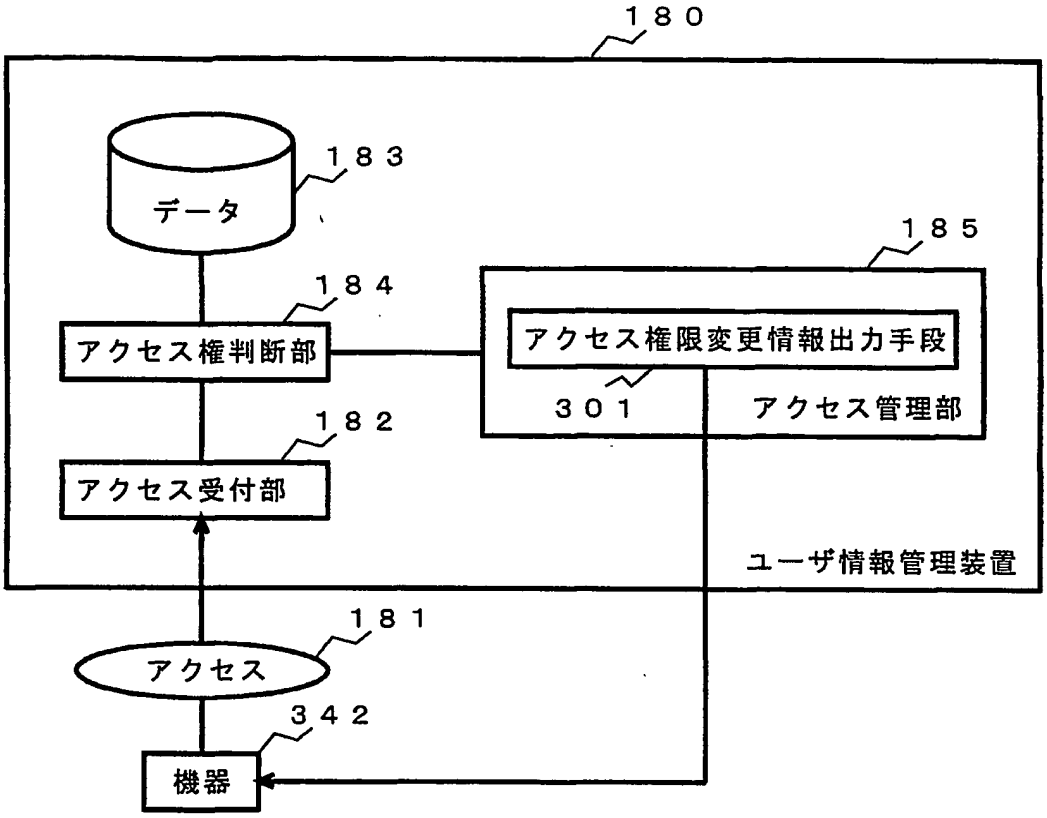
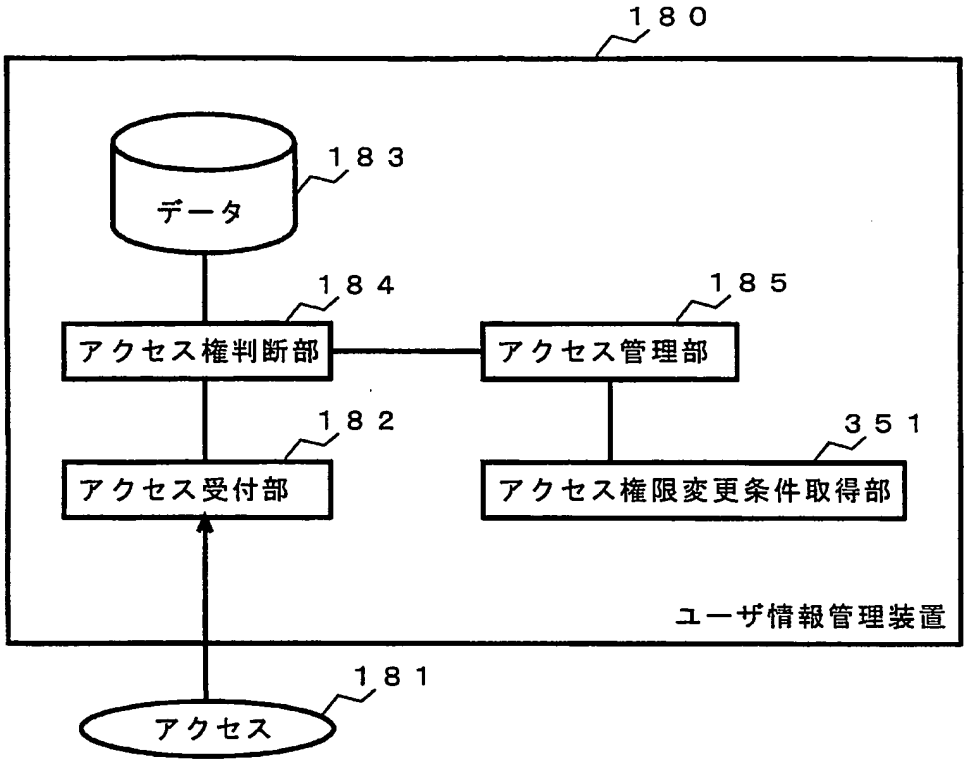

１８０
１８３
データ
１８５
１８４
アクセス権判断部
アクセス権限変更情報出力手段
３０１
アクセス管理部
１８２
アクセス受付部
ユーザ情報管理装置
１８１
アクセス
３４２
機器

図３５


１８０
１８３
データ
１８４
１８５
アクセス権判断部
アクセス管理部
１８２
３５１
アクセス受付部
アクセス権限変更条件取得部
ユーザ情報管理装置
１８１
アクセス

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/05655

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F15/00, G06F12/14, G06F12/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F15/00, G06F12/14, G06F12/00, G06F17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Toroku Jitsuyo Shinan Koho 1994-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 11-31019 A (Canon Inc.), 02 February, 1999 (02.02.99), Full text; all drawings (Family: none)	43-57 1-8,10,11, 15-22,24,25, 29-36,38,39
A		9,12-14,23, 26-28,37,40-42
Y	JP 6-83847 A (Hitachi, Ltd.), 25 March, 1994 (25.03.94), Full text; all drawings (Family: none)	1-8,10,11, 15-22,24,25, 29-36,38,39
A		9,12-14,23, 26-28,37,40-42
A	Masashi HASHIMOTO et al., "Network-jo deno Jouhou Tougou ni taisuru Privacy Hogo System no Arikata", Jouhou Shori Gakkai Kenkyu Houkoku, 30 January, 1999 (30.01.99), Vol.99, No.11, pages 17 to 24	9,23,37

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 September, 2001 (21.09.01)	02 October, 2001 (02.10.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/05655

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 10-240690 A (Hitachi, Ltd.), 11 September, 1998 (11.09.98), Full text; all drawings & US 6189032 B	14,28,42
A	JP 10-301857 A (NEC Corporation), 13 November, 1998 (13.11.98), Full text; all drawings (Family: none)	1-57
A	JP 5-324559 A (Olympus Optical Company Limited), 07 December, 1993 (07.12.93), Full text; all drawings (Family: none)	1-57
A	JP 1-243172 A (Hitachi, Ltd.), 27 September, 1989 (27.09.89), Full text; all drawings (Family: none)	1-57

国際調査報告

国際出願番号　PCT／JP01／05655

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ G06F15／00, G06F12／14, G06F12／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ G06F15／00, G06F12／14, G06F12／00, G06F17／60

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1926－1996年
日本国公開実用新案公報	1971－2001年
日本国実用新案登録公報	1996－2001年
日本国登録実用新案公報	1994－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y	JP　11－31019　A（キヤノン株式会社）2．2月．1999（02．02．99），全文，全図 （ファミリーなし）	43-57 1-8, 10, 11, 15-22, 24, 25, 29-36, 38, 39
A		9, 12-14, 23, 26-28, 37, 40-42
Y	JP　6－83847　A（株式会社日立製作所）25．3月．1994（25．03．94），全文，全図	1-8, 10, 11, 15-22, 24, 25,

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 21．09．01	国際調査報告の発送日 02.10.01
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 宮司　卓佳　5B　9555 電話番号　03－3581－1101　内線　3545

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　PCT／JP01／05655

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	（ファミリーなし）	29-36, 38, 39 9, 12-14, 23, 26-28, 37, 40-42
A	橋本誠志，金田重郎，ネットワーク上での情報統合に対するプライバシー保護システムのあり方，情報処理学会研究報告，３０．１月．１９９９（３０．０１．９９），第９９巻，第１１号，ｐ．１７－２４	9, 23, 37
A	ＪＰ　１０－２４０６９０　Ａ（株式会社日立製作所）１１．９月．１９９８（１１．０９．９８），全文，全図 ＆　ＵＳ　６１８９０３２　Ｂ	14, 28, 42
A	ＪＰ　１０－３０１８５７　Ａ（日本電気株式会社）１３．１１月．１９９８（１３．１１．９８），全文，全図 （ファミリーなし）	1-57
A	ＪＰ　５－３２４５５９　Ａ（オリンパス光学工業株式会社）７．１２月．１９９３（０７．１２．９３），全文，全図 （ファミリーなし）	1-57
A	ＪＰ　１－２４３１７２　Ａ（株式会社日立製作所）２７．９月．１９８９（２７．０９．８９），全文，全図 （ファミリーなし）	1-57